

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-091828  
 (43)Date of publication of application : 29.03.2002

---

(51)Int.Cl. G06F 12/14  
 G06F 1/00  
 G09C 1/00  
 G11B 20/10

---

(21)Application number : 2000-282720 (71)Applicant : SHARP CORP  
 (22)Date of filing : 18.09.2000 (72)Inventor : KAWA NORIAKI

---

(54) DATA PROCESSOR STORAGE DEVICE AND DATA TRANSFER SYSTEM USING THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To surely prevent data stored in a storage device from being illegally copied.

SOLUTION: A data processor 2 is provided with a processing part 21 for outputting an address for designating data to be processed by the data processor 2 in data stored in a storage device 1 and an encoder/decoder 22 for encoding the address outputted from the processing part 31 sending the encoded address to the storage device 1 receiving encoded data from the storage device 1 and decoding the encoded data. The encoder/decoder 22 is provided with setting parts (36 and 24) for receiving ID information peculiar to the storage device 1 from the storage device 1 and setting an initial value and logical operation on the basis of the ID information encoding/decoding KEY generating parts (25 and 27) for generating an encoding/decoding KEY by performing the set logical operation to the set initial value an encoding part 29 for encoding the address on the basis of the encoding/decoding KEY and a decoding part 28 for decoding the encoded data on the basis of the encoding/decoding KEY.

---

## CLAIMS

---

[Claim(s)]

[Claim 1] A treating part which outputs an address which specifies data which should be processed by said data processing device among data which is

removable data processing devices and was memorized by said memory storage in memory storage. Encipher said address outputted from said treating part and said enciphered address is sent to said memory storage. Receive data enciphered from said memory storage and have encryption/decryption machine which decrypts said enciphered data and said encryption/decryption machine. By receiving ID information peculiar to said memory storage from said memory storage and performing said set-up logical operation to a set part which sets up an initial value and a logical operation based on said ID information and said set-up initial value. A data processing device containing an encryption/decryption KEY generation part which generates encryption / decryption KEY. An encryption section which enciphers said address based on said encryption / decryption KEY and a decoding section which decrypts said enciphered data based on said encryption / decryption KEY.

[Claim 2] The data processing device according to claim 1 received in the state where said set part is not having said ID information enciphered when said data processing device is equipped with said memory storage.

[Claim 3] The data processing device according to claim 1 with which said encryption/decryption KEY generation part updates said encryption / decryption KEY periodically or irregularly.

[Claim 4] By performing an exclusive OR (EOR) operation to said encryption / decryption KEY and said address, said encryption section enciphers and said address said decoding section. The data processing device according to claim 1 which decrypts said enciphered data by performing an exclusive OR (EOR) operation to said encryption / decryption KEY and said enciphered data.

[Claim 5] The data processing device comprising according to claim 1:  
A shift register to which said encryption/decryption KEY generation part holds data containing two or more bits and said data is shifted according to a shift clock.  
A feedback equivalent logic formation part which performs an alternative exclusive OR (EOR) operation according to said set-up logical operation to said data currently held at said shift register and feeds back the result of an operation to an input of said shift register.

[Claim 6] The data processing device according to claim 5 which generates said encryption / decryption KEY when said encryption/decryption KEY generation part rearranges bit order of said data currently held at said shift register in the given order.

[Claim 7] The data processing device according to claim 5 which generates new encryption / decryption KEY when said encryption/decryption KEY generation part changes the number of times which shifts said data currently held at said shift register.

[Claim 8] Memory storage which can be desorbed to a data processing device characterized by comprising the following.

A storage parts store which is a storage parts store data was remembered to be and outputs data corresponding to an address.

Receive an address enciphered from said data processing device and said enciphered address is decrypted. Encipher said data outputted from said memory storage have encryption/decryption machine which sends said enciphered data to said data processing device and said encryption/decryption machine. An encryption/decryption KEY generation part which generates encryption / decryption KEY based on ID information peculiar to said memory storage beforehand set as said memory storage.

A decoding section which decrypts said enciphered address based on said encryption / decryption KEY.

An encryption section which enciphers said data outputted from said memory storage based on said encryption / decryption KEY.

[Claim 9] The memory storage according to claim 8 with which said encryption/decryption KEY generation part updates said encryption / decryption KEY periodically or irregularly.

[Claim 10] Said decoding section by performing an exclusive OR (EOR) operation to said encryption / decryption KEY and said enciphered address. The memory storage according to claim 8 which enciphers said data when said enciphered address is decrypted and said encryption section performs an exclusive OR (EOR) operation to said encryption / decryption KEY and said data.

[Claim 11] The memory storage comprising according to claim 8:

A shift register to which said encryption/decryption KEY generation part holds data containing two or more bits and said data is shifted according to a shift clock. A feedback part which performs an alternative exclusive OR (EOR) operation beforehand set up based on said ID information to said data currently held at said shift register and feeds back the result of an operation to an input of said shift register.

[Claim 12] The memory storage according to claim 11 with which said data currently held at said shift register is initialized by initial value beforehand set up based on said ID information.

[Claim 13] The memory storage according to claim 11 which generates said encryption / decryption KEY when said encryption/decryption KEY generation part rearranges bit order of said data currently held at said shift register in the given order.

[Claim 14] The memory storage according to claim 11 which generates new encryption / decryption KEY when said encryption/decryption KEY generation part changes the number of times which shifts said data currently held at said shift register.

[Claim 15] The memory storage according to claim 8 currently formed on a semiconductor chip with single said storage parts store and said encryption/decryption machine.

[Claim 16] Are a data processing device and memory storage removable to said data processing device the data transfer system which it had and said data

processing deviceA treating part which outputs an address which specifies data which should be processed by said data processing device among data memorized by said memory storageEncipher said address outputted from said treating partand said enciphered address is sent to said memory storageReceive data enciphered from said memory storagehave 1st encryption/decryption machine that decrypts said enciphered dataand said 1st encryption/decryption machineBy receiving ID information peculiar to said memory storage from said memory storageand performing said set-up logical operation to a set part which sets up an initial value and a logical operation based on said ID informationand said set-up initial valueThe 1st encryption/decryption KEY generation part that generates the 1st encryption / decryption KEYIt is the storage parts storeas for said memory storagedata was remembered to be including the 1st encryption section that enciphers said address based on said the 1st encryption / decryption KEYand the 1st decoding section that decrypts said enciphered data based on said the 1st encryption / decryption KEYA storage parts store which outputs data corresponding to said addressand an address enciphered from said data processing device are receivedDecrypt said enciphered address and said data outputted from said memory storage is encipheredHave 2nd encryption/decryption machine that sends said enciphered data to said data processing deviceand said 2nd encryption/decryption machineThe 2nd encryption/decryption KEY generation part that generates the 2nd encryption / decryption KEY based on ID information peculiar to said memory storage beforehand set as said memory storageA data transfer system containing the 2nd decoding section that decrypts said enciphered address based on said the 2nd encryption / decryption KEYand the 2nd encryption section that enciphers said data outputted from said memory storage based on said the 2nd encryption / decryption KEY.

[Claim 17]The data transfer system according to claim 16 generated according to logic with equivalent said the 1st encryption / decryption KEYand said the 2nd encryption/decryption KEY.

[Claim 18]The data transfer system according to claim 16 with which said data processing device is further provided with a control section which controls said 1st encryption/decryption machine and said 2nd encryption/decryption machine at least.

[Claim 19]When said data processing device is equipped with said memory storagesaid control sectionSo that said the 1st encryption / decryption KEYand said the 2nd encryption/decryption KEY may be reset and said the 1st same encryption / decryption KEYand said the 2nd encryption/decryption KEY may be generated based on said ID informationThe data transfer system according to claim 18 which controls said 1st encryption/decryption machine and said 2nd encryption/decryption machine.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the data processing device and memory storage which prevent the program memorized by memory storage removable to a data processing device and data from being reproduced unjustly and a data transmission system.

[0002]

[Description of the Prior Art] The dismountable semiconductor memory device (for example ROM) is supplied to the commercial scene in large quantities in the form of a home video game cassette etc. from the data processing device today. Supposing it does not take the measure against unjust copy protection there is a possibility that the pirate edition of a game cassette may appear on the market in a commercial scene in large quantities.

[0003] How to prevent the data memorized by the semiconductor memory device from being reproduced unjustly conventionally Or using the data reproduced unjustly as a method of making it impossible or difficult (1) Before reading the method of memorizing the enciphered data to a semiconductor memory device and the data memorized by (2) semiconductor memory device the method of performing performs authentication which checks that a semiconductor memory device or a data processing device is regular is known.

[0004] For example JPS60-167033A JPS61-67136A and JPH5-53921A are indicating the method of memorizing the enciphered data to a semiconductor memory device.

[0005] For example after performing performs authentication which checks that JPH6-168185A and the patent No. 2698371 gazette have a regular data processing device with which it is equipped with a semiconductor memory device the method of reading the data memorized by the semiconductor memory device is indicated.

[0006]

[Problem(s) to be Solved by the Invention] In the method of memorizing the enciphered data to a semiconductor memory device since the data itself memorized by the semiconductor memory device is enciphered the change use of data and the surreptitious use of a program which were read from the semiconductor memory device can be prevented. However in this method the enciphered data which is memorized by the semiconductor memory device cannot be prevented from being reproduced unjustly.

[0007] In the method of performing performs authentication which checks a data processing device being regular the data memorized by the semiconductor memory device using the data processing device which is not regular can be prevented from being reproduced unjustly. However in this method since it is possible observing and (probe) reading the data which is transmitted between a semiconductor memory device and a data processing device and which is not enciphered cannot prevent certainly surreptitious use of the data memorized by the semiconductor memory device and a program.

[0008] How to encipher communications on the opened networks such as wireless

information communication is also known. For example JPH6-342257A and JPH8-307411A. Encryption / decryption KEY (key) is generated based on the pseudo-random number which made it generate combining LFSR (linear feedback shift register) and the method of enciphering commo data based on this encryption / decryption KEY (key) is indicated. Encoding technology given in these gazettes is the art about secret communication. Using such encoding technology for the purpose of preventing the data memorized by the semiconductor memory device from being reproduced unjustly is not suggested to these gazettes.

[0009] This invention is made in order to solve the problem mentioned above and it is a thing.

the purpose is to provide the data processing device and memory storage which prevent the program which is alike and is memorized by removable memory storage and data from being reproduced unjustly and a data transmission system.

[0010]

[Means for Solving the Problem] A treating part which outputs an address which specifies data in which a data processing device of this invention should be processed by said data processing device in memory storage among data which is removable data processing devices and was memorized by said memory storage. Encipher said address outputted from said treating part and said enciphered address is sent to said memory storage. Receive data enciphered from said memory storage. Have encryption/decryption machine which decrypts said enciphered data and said encryption/decryption machine. By receiving ID information peculiar to said memory storage from said memory storage and performing said set-up logical operation to a set part which sets up an initial value and a logical operation based on said ID information and said set-up initial value. An encryption/decryption KEY generation part which generates encryption / decryption KEY and an encryption section which enciphers said address based on said encryption / decryption KEY. Thereby the above-mentioned purpose is attained including a decoding section which decrypts said enciphered data based on said encryption / decryption KEY.

[0011] Said set part may be received in the state where said ID information is enciphered when said data processing device is equipped with said memory storage.

[0012] Said encryption/decryption KEY generation part may update said encryption / decryption KEY periodically or irregularly.

[0013] By performing an exclusive OR (EOR) operation to said encryption / decryption KEY and said address, said encryption section enciphers and said address said decoding section. Said enciphered data may be decrypted by performing an exclusive OR (EOR) operation to said encryption / decryption KEY and said enciphered data.

[0014] A shift register to which said encryption/decryption KEY generation part holds data containing two or more bits and said data is shifted according to a shift clock. An alternative exclusive OR (EOR) operation according to said set-up logical operation may be performed to said data currently held at said shift register and a feedback equivalent logic formation part which feeds back the result of an

operation to an input of said shift register may be included.

[0015] Said encryption/decryption KEY generation part may generate said encryption / decryption KEY by rearranging bit order of said data currently held at said shift register in the given order.

[0016] Said encryption/decryption KEY generation part may generate new encryption / decryption KEY by changing the number of times which shifts said data currently held at said shift register.

[0017] A storage parts store which memory storage of this invention is the memory storage which can be desorbed to a data processing device is a storage parts store data was remembered to be and outputs data corresponding to an address. Receive an address enciphered from said data processing device and said enciphered address is decrypted. Encipher said data outputted from said memory storage have encryption/decryption machine which sends said enciphered data to said data processing device and said encryption/decryption machine. An encryption/decryption KEY generation part which generates encryption / decryption KEY based on ID information peculiar to said memory storage beforehand set as said memory storage. Thereby the above-mentioned purpose is attained including a decoding section which decrypts said enciphered address based on said encryption / decryption KEY and an encryption section which enciphers said data outputted from said memory storage based on said encryption / decryption KEY.

[0018] Said encryption/decryption KEY generation part may update said encryption / decryption KEY periodically or irregularly.

[0019] Said decoding section by performing an exclusive OR (EOR) operation to said encryption / decryption KEY and said enciphered address. Said encryption section may encipher said data by decrypting said enciphered address by performing an exclusive OR (EOR) operation to said encryption / decryption KEY and said data.

[0020] A shift register to which said encryption/decryption KEY generation part holds data containing two or more bits and said data is shifted according to a shift clock. An alternative exclusive OR (EOR) operation beforehand set up based on said ID information to said data currently held at said shift register may be performed and a feedback part which feeds back the result of an operation to an input of said shift register may be included.

[0021] Said data currently held at said shift register may be initialized by initial value beforehand set up based on said ID information.

[0022] Said encryption/decryption KEY generation part may generate said encryption / decryption KEY by rearranging bit order of said data currently held at said shift register in the given order.

[0023] Said encryption/decryption KEY generation part may generate new encryption / decryption KEY by changing the number of times which shifts said data currently held at said shift register.

[0024] It may be formed on a semiconductor chip with single said storage parts store and said encryption/decryption machine.

[0025] A data transfer system of this invention is a data processing device and memory storage removable to said data processing device a data transfer system which it had and said data processing device a treating part which outputs an address which specifies data which should be processed by said data processing device among data memorized by said memory storage. Encipher said address outputted from said treating part and said enciphered address is sent to said memory storage. Receive data enciphered from said memory storage. Have 1st encryption/decryption machine that decrypts said enciphered data and said 1st encryption/decryption machine. By receiving ID information peculiar to said memory storage from said memory storage and performing said set-up logical operation to a set part which sets up an initial value and a logical operation based on said ID information and said set-up initial value. The 1st encryption/decryption KEY generation part that generates the 1st encryption / decryption KEY. It is the storage parts store as for said memory storage data was remembered to be including the 1st encryption section that enciphers said address based on said the 1st encryption / decryption KEY and the 1st decoding section that decrypts said enciphered data based on said the 1st encryption / decryption KEY. A storage parts store which outputs data corresponding to said address and an address enciphered from said data processing device are received. Decrypt said enciphered address and said data outputted from said memory storage is enciphered. Have 2nd encryption/decryption machine that sends said enciphered data to said data processing device and said 2nd encryption/decryption machine. The 2nd encryption/decryption KEY generation part that generates the 2nd encryption / decryption KEY based on ID information peculiar to said memory storage beforehand set as said memory storage. Thereby the above-mentioned purpose is attained including the 2nd decoding section that decrypts said enciphered address based on said the 2nd encryption / decryption KEY and the 2nd encryption section that enciphers said data outputted from said memory storage based on said the 2nd encryption / decryption KEY.

[0026] It may be generated according to logic with equivalent said the 1st encryption / decryption KEY and said the 2nd encryption/decryption KEY.

[0027] Said data processing device may be further provided with a control section which controls said 1st encryption/decryption machine and said 2nd encryption/decryption machine at least.

[0028] When said data processing device is equipped with said memory storage said control section so that said the 1st encryption / decryption KEY and said the 2nd encryption/decryption KEY may be reset and said the 1st same encryption / decryption KEY and said the 2nd encryption/decryption KEY may be generated based on said ID information. Said 1st encryption/decryption machine and said 2nd encryption/decryption machine may be controlled.

[0029]

[Embodiment of the Invention] Hereafter an embodiment of the invention is described referring to Drawings.

[0030] Drawing 1 shows the example of composition of the data transfer system



100 of an embodiment of the invention.

[0031]The data transfer system 100 is provided with the following.

Memory storage 1.

Data processing device 2.

The memory storage 1 is constituted by the data processing device 2 removable. The data processing device 2 is equipped with the one memory storage 1 chosen from two or more memory storage of the same standard.

[0032]The data processing device 2 outputs the address enciphered by the memory storage 1 with which it was equipped. The memory storage 1 outputs the enciphered data corresponding to the enciphered address to the data processing device 2. Thus it becomes difficult to get to know the contents of the data memorized by the memory storage 1 from data transmitting by enciphering the address and data which are transmitted between the memory storage 1 and the data processing device 2.

[0033]The memory storage 1 is the game cassette for home video games in which a game program and various data were memorized for example. The data processing device 2 is a home video game machine for example. The home video game machine has an opening for equipping with a game cassette. If the opening of a home video game machine is equipped with a game cassette the game program and various data which are memorized by the game cassette will be read to a home video game machine and a game screen will be displayed on the display of the television etc. which are connected to the home video game machine.

[0034]The memory storage 1 is provided with the following.

Storage parts store 10.

Encryption/decryption machine 11.

As for the storage parts store 10 and encryption/decryption machine 11 it is preferred to be formed on a single semiconductor chip (for example silicon chip).

[0035]ID information (for example ID number) peculiar to the memory storage 1 and a program and various data are beforehand memorized by the storage parts store 10. ID information is a lot number assigned to every [ of the same standard ] memory storage (product) for example. Or ID information may be the value chosen from two or more values. ID information is memorized to the predetermined address (for example 0th street) of the storage parts store 10. The storage parts store 10 receives an address from encryption/decryption machine 11 and outputs the data memorized by the position corresponding to the address to encryption/decryption machine 11.

[0036]In this Description the term "data" is understood as a comprehensive term which shall mean the information arbitrary type which may be memorized by the storage parts store 10 and contains a program and various data.

[0037]Encryption/decryption machine 11 receives the enciphered address from the data processing device 2 and generates an address by decrypting the enciphered address. The address is outputted to the storage parts store 10.

Encryption/decryption machine 11 receives the data outputted from the storage parts store 10 and generates the data enciphered by enciphering the data. The

enciphered data is outputted to the data processing device 2.

[0038]The data processing device 2 is provided with the following.

Treating part 21.

Encryption/decryption machine 22.

[0039]If the data processing device 2 is equipped with the memory storage 1 encryption/decryption machine 11 in the memory storage 1 and encryption/decryption machine 22 in the data processing device 2 will be in the state where it was electrically connected mutually. For example encryption/decryption machine 11 and encryption/decryption machine 22 of each other may electrically be connected via a connector (not shown).

[0040]The treating part 21 outputs the address which specifies the data which should be processed by the data processing device 2 among the data memorized by the memory storage 1.

[0041]Encryption/decryption machine 22 receives the address outputted from the treating part 21 and generates the address enciphered by enciphering the address. The enciphered address is outputted to the memory storage 1.

Encryption/decryption machine 22 receives the enciphered data which was outputted from the memory storage 1 and generates data by decrypting the enciphered data. The data is outputted to the treating part 21.

[0042]The data processing device 2 contains further the control section 20 which controls encryption/decryption machine 11 encryption/decryption machine 22 and the treating part 21.

[0043]The control section 20 contains the code generation controller 23. The code generation controller 23 so that the timing of generation of the encryption / decryption KEY in encryption/decryption machine 11 the timing of change and generation of the encryption / decryption KEY in encryption/decryption machine 22 and change may synchronize Encryption/decryption machine 11 and encryption/decryption machine 22 are controlled.

[0044]The code generation controller 23 supplies a control signal common to encryption/decryption machine 11 and encryption/decryption machine 22 to encryption/decryption machine 11 and encryption/decryption machine 22 via the controlling signal line 41 The control signal only relevant to encryption/decryption machine 22 is supplied to encryption/decryption machine 22 via the controlling signal line 42.

[0045]Drawing 2 shows the example of composition of encryption/decryption machine 11 of the memory storage 1.

[0046]Encryption/decryption machine 11 contains LFSR (Linear Feedback Shift Register) 12 which generates a pseudo-random number.

[0047]LFSR 12 is a circuit which performs an exclusive OR (below Exclusive OR; calls it "EOR") operation to the bit of shoes to be chosen among the data of N bit currently held at the shift register and feeds back the result of an operation to the input of a shift register. A shift register is constituted by connecting a D flip-flop (DFF) in series for example.

[0048] a maximum of [ from which the characteristic differs by whether the result of an operation is fed back to which bit position of a shift register by performing an EOR operation to which bit among the data of N bit currently held at the shift register ] -- the pseudorandom-numbers (pattern) sequence of the cycle of  $2^N-1$  can be acquired. Here generally the pseudo-random number sequence which has a cycle of  $2^N-1$  which is the maximum is called "an M sequence (Maximum length Sequences)." Here N is two or more arbitrary integers.

[0049] The Nth polynomial shown in (several 1) can express whether an EOR operation is performed to which bit among the data of N bit currently held at the shift register.

[0050]

[Equation 1]

$$f(x) = x^N + a_{N-1}x^{N-1} + \dots + a_1x + a_0$$

However it is referred to as  $a_k=0$  when not using the k-th bit for an EOR operation among data of N bit currently held at a shift register when using the k-th bit for an EOR operation among data of N bit currently held at a shift register. It is referred to as  $a_0=1$  and  $a_N=1$ . This polynomial  $f(x)$  is called a LFSR characteristic polynomial and expresses the characteristic of pseudorandom numbers which LFSR generates.

[0051] For example when performing an EOR operation to the 1st bit and the 4th bit in the case of N=4 LFSR characteristic polynomial  $f(x)$  is expressed as " $x^4+x+1$ ."

[0052] Although a LFSR characteristic polynomial for forming an M sequence is restricted in this invention, pseudo-random number sequence in particular acquired does not need to be an M sequence. However as an initial value of data of N bit held at a shift register, setting up a value (for example 0...0 (ALL0)) which causes a dead loop (or stack State) from which change does not take place to data of N bit held at a shift register even if it repeats this processing must be avoided.

[0053] Based on ID information memorized by the storage parts store 10, an initial value and a LFSR characteristic polynomial of data of N bit which should be held at a shift register of LFSR are determined beforehand. LFSR12 is formed as a circuit which fills an initial value and a LFSR characteristic polynomial of data of the N bit determined beforehand.

[0054] Drawing 3 shows an example of composition of LFSR12. LFSR12 has the shift register 18a holding data of N bit. The shift register 18a comprises N D flip-flops (DFF) 18 connected in series.

[0055] If an initial value load signal is inputted into LFSR12, data of N bit currently held at the shift register 18a will be initialized. An initial value of data of the N bit is beforehand memorized by the N registers 19. An initial value of data of the N bit is beforehand determined based on ID information memorized by the storage parts store 10. Or an initial value of data of the N bit is beforehand determined by an initial value load signal inputted into each bit of N DFF 18 being connected to either an asynchronous set which is each bit or asynchronous reset.

[0056]If a shift clock is inputted into LFSR12 1 bit of data of N bit currently held at the shift register 18a will be shifted in the direction of every predetermined one by one. The number of times of a shift can be set as the arbitrary number of times.

[0057]A bit of some of the data of N bit currently held at the shift register 18a in accordance with a selection rule beforehand determined based on ID information memorized by the storage parts store 10 is chosen and an EOR operation is performed to a selected bit. A result of the EOR operation is fed back to an input of the 1st bit (namely the 1st step of DFF18) of the shift register 18a. In an example shown in drawing 3 an EOR operation is performed to the 1st bit and the 3rd bit among data of N bit currently held at the shift register 18a and a result of the EOR operation is fed back to an input which is the 1st bit of the shift register 18a. The EOR arithmetic element 13 is used in order to perform an EOR operation to the 1st bit and the 3rd bit.

[0058]A selection rule which specifies whether which bit of an initial value of data of N bit held at the shift register 18a and the data of N bit held at the shift register 18a is chosen and an EOR operation is performed is uniquely determined based on ID information memorized by the storage parts store 10.

[0059]Synchronizing with a shift clock with which LFSR12 is supplied from the code generation controller 23 only the number of operation times M set up at random repeats shift operation and an EOR operation of the shift register 18a. Data of N bit outputted from N DFF18 contained in the shift register 18a is outputted from LFSR12 as the output data OUT after an end of repetition processing. The output data OUT expresses a pseudo-random number.

[0060]Again with reference to drawing 2 the register (Key\_Reg) 14 is connected to LFSR12 so that bit order of the output data OUT outputted from LFSR12 may be rearranged into predetermined bit order. Data of N bit held Key\_Reg14 is considered as encryption / decryption KEY.

[0061]Bit width of the output data OUT and bit width of Key\_Reg14 which are outputted from LFSR12 are the same as the larger one among bit width of data outputted from bit width and the storage parts store 10 of an address which are inputted into the storage parts store 10 or it has become more than it. Therefore data of a bit chosen among data of N bit held Key\_Reg14 according to bit width of an address or bit width of data may be considered as encryption / decryption KEY.

[0062]A KEY reset signal and a KEY set clock are supplied to Key\_Reg14 from the code generation controller 23. Synchronizing with a KEY reset signal the encryption / decryption KEY currently held Key\_Reg14 are reset. Synchronizing with a KEY set clock the output data OUT outputted from LFSR12 is incorporated into Key\_Reg14 and is held.

[0063]A KEY set clock is outputted periodically or irregularly from the code generation controller 23. Encryption / decryption KEY answers a KEY set clock and is updated periodically or irregularly.

[0064]Thus LFSR12 and Key\_Reg14 function based on ID information peculiar to the memory storage 1 beforehand set as the memory storage 1 as an

encryption/decryption KEY generation part which generates encryption / decryption KEY.

[0065]The encryption / decryption KEY held Key\_Reg14 are given to the decryption EOR gate sequence 15 and the encryption EOR gate sequence 17.

[0066]The decryption EOR gate sequence 15 receives an enciphered address from the data processing device 2. An enciphered address is decrypted by receiving encryption / decryption KEY from Key\_Reg14 and performing an EOR operation to each bit of an address and each bit of encryption / decryption KEY which were enciphered.

[0067]Thus the decryption EOR gate sequence 15 functions as a decoding section which decrypts an address enciphered based on encryption / decryption KEY.

[0068]The EOR result of an operation by the decryption EOR gate sequence 15 is given to the selector 16. The selector 16 refers to the encryption / decryption KEY currently held Key\_Reg14. When encryption / decryption KEY is "ALL0" (state where all bit is "0" and encryption / decryption KEY is not set up) The 0th address is outputted to the storage parts store 10 and when encryption / decryption KEY is not "ALL0" an address outputted from the decryption EOR gate sequence 15 is outputted to the storage parts store 10.

[0069]The storage parts store 10 outputs data stored in a position corresponding to an address outputted from the selector 16.

[0070]The encryption EOR gate sequence 17 receives data outputted from the storage parts store 10. Data outputted from the storage parts store 10 is enciphered by receiving encryption / decryption KEY from Key\_Reg14 and performing an EOR operation to each bit of data and each bit of encryption / decryption KEY which were outputted from the storage parts store 10.

[0071]Thus the encryption EOR gate sequence 17 functions as an encryption section which enciphers data outputted from the storage parts store 10 based on encryption / decryption KEY.

[0072]As mentioned above when the encryption / decryption KEY currently held Key\_Reg14 are "ALL0" the selector 16 outputs "the 0th address" to the storage parts store 10 irrespective of an address outputted from the decryption EOR gate sequence 15. The storage parts store 10 outputs ID information memorized by "the 0th street" to "the 0th address." In this case the encryption EOR gate sequence 17 will perform an EOR operation to "ALL0" and ID information. As a result ID information is outputted from the encryption EOR gate sequence 17.

[0073]Drawing 4 shows an example of composition of encryption/decryption machine 22 of the data processing device 2.

[0074]The register (ID\_Reg) 36 holding ID information to which encryption/decryption machine 22 was outputted from the memory storage 1. Based on ID information held ID\_Reg36 the LFSR initial value characteristic polynomial set part 24 which determines an initial value and a LFSR characteristic polynomial for generating a pseudo-random number is included.

[0075]If the data processing device 2 is equipped with the memory storage 1 ID information will be transmitted to the data processing device 2 from the memory

storage 1. This ID information is transmitted in the state where it is not enciphered.

[0076]ID\_Reg36 incorporates and holds ID information transmitted from the memory storage 1 synchronizing with ID set signal supplied from the code generation controller 23. ID information held ID\_Reg36 is outputted to the LFSR initial value characteristic polynomial set part 24.

[0077]Logic used when determining an initial value and a LFSR characteristic polynomial for generating a pseudo-random number based on ID information in the LFSR initial value characteristic polynomial set part 24In LFSR12 provided in encryption/decryption machine 11 of the memory storage 1it is equivalent to logic used when determining beforehand an initial value and a LFSR characteristic polynomial for generating a pseudo-random number based on ID information. As opposed to a circuit which realizes an initial value and a LFSR characteristic polynomial for generating a pseudo-random number beforehand determined based on ID information being made from LFSR12 in LFSR12In the LFSR initial value characteristic polynomial set part 24the control signal SELBUS which shows an initial value and a LFSR characteristic polynomial for generating a pseudo-random number determined based on ID information is outputted to LFSR25.

[0078]LFSR25 is provided with the following.

Shift register 30.

LFSR feedback equivalent logic formation part 31.

[0079]Drawing 5 (a) shows an example of composition of the shift register 30 and the LFSR feedback equivalent logic formation part 31.

[0080]An initial value for generating a pseudo-random number determined by the LFSR initial value characteristic polynomial set part 24 is set as the shift register 30 as an initial value of data of N bit held at the shift register 30.

[0081]The LFSR feedback equivalent logic formation part 31 has two or more gate elements 33 for LFSR feedback equivalent logic formation for forming a logic synthesis gate equivalent to a LFSR characteristic polynomial. Each of two or more gate elements 33 for LFSR feedback equivalent logic formation is provided with the following.

Input terminal A.

Input terminal B.

Output terminal Y.

Select signal input terminal S.

[0082]Drawing 5 (b) shows an example of composition of the gate element 33 for LFSR feedback equivalent logic formation. The gate element 33 for LFSR feedback equivalent logic formation is provided with the following.

EOR arithmetic element 34.

The 4-1 selector 35.

[0083]The 4-1 selector 35 chooses one of four input signals according to a select

signal inputted into the select signal input terminal S. Four input signals are a signal which shows a result of having performed an EOR operation by the EOR arithmetic element 34 to a signal inputted from the input terminal Aa signal inputted from the input terminal Ba signal inputted from the input terminal Aand a signal inputted from the input terminal Band a signal which shows the logic phi. A signal with the 4-1 selected selector 35 is outputted from the output terminal Y.

[0084]A select signal is a part of control signal SELBUS outputted from the LFSR initial value characteristic polynomial set part 24. A select signal is based on a LFSR characteristic polynomial determined by the LFSR initial value characteristic polynomial set part 24.

[0085]Again with reference to drawing 5 (a)the LFSR feedback equivalent logic formation part 31 contains two or more gate elements 33 for LFSR feedback equivalent logic formation arranged by two or more pyramid type hierarchies. The  $N/2$  gate elements 33 for LFSR feedback equivalent logic formation are located in a line with two or more of the hierarchies' least significant layer in parallelAn output from the output terminal Y of the two adjoining gate elements 33 for LFSR feedback equivalent logic formation is inputted into the input terminal A and the input terminal B of the gate element 33 for LFSR feedback equivalent logic formation of the upper layer.

[0086]The LFSR feedback equivalent logic formation part 31 sets an initial value for generating a pseudo-random number determined by the LFSR initial value characteristic polynomial set part 24 synchronizing with an initial value load signal supplied from the code generation controller 23 as the shift register 30.

[0087]The shift register 30 comprises N D flip-flops (DFF) 32 with set-reset connected in series.

[0088]If a shift clock is inputted into the shift register 301 bit of data of N bit currently held at the shift register 30 will be shifted in the direction of every predetermined one by one. For examplea bit currently held DFF32 of eye watch (K+1) is shifted to DFF32 of eye watch (K+2) at the same time a bit currently held the Kth DFF32 is shifted to DFF32 of eye watch (K+1) synchronizing with a shift clock. Thussynchronizing with a shift clockall the bits of data held at the shift register 30 are shifted simultaneously.

[0089]Each of output signal SOUT (1) - (N) outputted from N DFF32 is inputted into the gate element 33 for LFSR feedback equivalent logic formation arranged at a least significant layer of the LFSR feedback equivalent logic formation part 31. For examplethe output signal SOUT (1) and (2) is inputted into the input terminal A and the input terminal B of the gate element 33 for LFSR feedback equivalent logic formationrespectively. According to a select signal inputted into the select signal input terminal S of the gate element 33 for LFSR feedback equivalent logic formationone of four signals inputted into the 4-1 selector 35 is chosen. A selected signal is outputted from the output terminal Y of the gate element 33 for LFSR feedback equivalent logic formation. A signal outputted from the output terminal Y of the gate element 33 for LFSR feedback equivalent logic formation is inputted into the input terminal A or the input terminal B of the gate element 33

for LFSR feedback equivalent logic formation of the upper layer. Such processing is repeated toward a top layer of the LFSR feedback equivalent logic formation part 31. As a result 1 bit is outputted from the one gate element 33 for LFSR feedback equivalent logic formation of a top layer. This value of 1 bit is fed back to an input of the 1st bit (namely the 1st step of DFF32) of the data of N bit held at the shift register 30 as the control signal FBIN.

[0090] Synchronizing with a shift clock with which the shift register 30 is supplied from the code generation controller 23 only the number of operation times M set up at random repeats shift operation and an EOR operation of the shift register 30. Data of N bit outputted from N DFF32 contained in the shift register 30 is outputted from LFSR25 as output data SOUT after an end of repetition processing. Output data SOUT expresses a pseudo-random number.

[0091] A shift clock inputted into the shift register 30 is the same signal as a shift clock inputted into LFSR12.

[0092] Thus LFSR25 generates a pseudo-random number equivalent to a pseudo-random number generated by LFSR12 according to a logical operation equivalent to a logical operation in LFSR12.

[0093] The number of times M of shift operation carried out in order to generate pseudorandom numbers in LFSR25 and LFSR12 is set up at random by the code generation controller 23. The number of times M of shift operation is set up based on time clocked by a timer for example.

[0094] Again with reference to drawing 4 the register (Key\_Reg) 27 is connected to LFSR25 so that bit order of output data SOUT outputted from LFSR25 may be rearranged into predetermined bit order. Data of N bit held Key\_Reg27 is considered as encryption / decryption KEY.

[0095] Bit width of output data SOUT and bit width of Key\_Reg27 which are outputted from LFSR25 are the same as the larger one among bit width of data inputted into bit width and the treating part 21 of an address which are outputted from the treating part 21 or it has become more than it. Therefore data of a bit chosen among data of N bit held Key\_Reg27 according to bit width of an address or bit width of data may be considered as encryption / decryption KEY.

[0096] A KEY reset signal and a KEY set clock are supplied to Key\_Reg27 from the code generation controller 23. Synchronizing with a KEY reset signal the encryption / decryption KEY currently held Key\_Reg27 are reset. Synchronizing with a KEY set clock output data SOUT outputted from LFSR25 is incorporated into Key\_Reg27 and is held.

[0097] A KEY set clock inputted into Key\_Reg27 is the same signal as a KEY set clock inputted into Key\_Reg14.

[0098] Thus ID\_Reg36 and the LFSR initial value characteristic polynomial set part 24 function as a set part which sets up an initial value and a logical operation based on ID information peculiar to the memory storage 1. LFSR25 and Key\_Reg27 function by performing a logical operation set up to a set-up initial value as an encryption/decryption KEY generation part which generates encryption / decryption KEY.



[0099]The encryption / decryption KEY held Key\_Reg27 are given to the decryption EOR gate sequence 28 and the encryption EOR gate sequence 29.

[0100]The decryption EOR gate sequence 28 receives enciphered data from the memory storage 1. Enciphered data is decrypted by receiving encryption / decryption KEY from Key\_Reg27 and performing an EOR operation to each bit of data and each bit of encryption / decryption KEY which were enciphered.

[0101]Thus the decryption EOR gate sequence 28 functions as a decoding section which decrypts data enciphered based on encryption / decryption KEY.

[0102]The encryption EOR gate sequence 29 receives an address outputted from the treating part 21. An address outputted from the treating part 21 is enciphered by receiving encryption / decryption KEY from Key\_Reg27 and performing an EOR operation to each bit of an address and each bit of encryption / decryption KEY which were outputted from the treating part 21.

[0103]Thus the encryption EOR gate sequence 29 functions as an encryption section which enciphers an address outputted from the treating part 21 based on encryption / decryption KEY.

[0104]Next with reference to drawing 6 operation of the data transfer system 100 containing the memory storage 1 and the data processing device 2 is explained.

[0105]Hard reset will be performed if the data processing device 2 is equipped with the memory storage 1. This hard reset is answered and the code generation controller 23 of the control section 20 is outputted to Key\_Reg27 in which a "KEY reset signal" was formed by encryption/decryption machine 22 and Key\_Reg14 which were provided in encryption/decryption machine 11 (drawing 6 (b)). As a result data held Key\_Reg14 and Key\_Reg27 is reset by "ALL0" respectively (drawing 6 (a)). It is shown that it is in a state where encryption / decryption KEY was reset that data held Key\_Reg14 and Key\_Reg27 is "ALL0."

[0106]If "ALL0" is held Key\_Reg14 the selector 16 will output "the 0th address" to the storage parts store 10 irrespective of an address outputted from the decryption EOR gate sequence 15.

[0107]The storage parts store 10 outputs ID information memorized to "the 0th address." ID information is transmitted to the data processing device 2 via the encryption EOR gate sequence 17.

[0108]Thus in the state where encryption / decryption KEY was reset there is no possibility that data may be read from addresses "other than 0th" by associating "the 0th street" of the state where encryption / decryption KEY was reset and the storage parts store 10. [ of the storage parts store 10 ]

[0109]The code generation controller 23 of the control section 20 outputs "ID set signal" to ID\_Reg36 (drawing 6 (i)). as a result ID information transmitted to the data processing device 2 from the memory storage 1 sets to ID\_Reg36 -- having (drawing 6 (h)) -- it is outputted to the LFSR initial value characteristic polynomial set part 24.

[0110]The LFSR initial value characteristic polynomial set part 24 determines an initial value and a LFSR characteristic polynomial for generating a pseudo-random number based on ID information (drawing 6 (g)). The LFSR initial value

characteristic polynomial set part 24 outputs the control signal SELBUS for setting up an initial value and a LFSR characteristic polynomial for generating a pseudo-random number to the LFSR feedback equivalent logic formation part 31.

[0111]The code generation controller 23 of the control section 20 outputs an "initial value load signal" to LFSR12 and LFSR25 (drawing 6 (e)).

[0112]An "initial value load signal" is answered and an initial value is set as the shift register 18a of LFSR12 and an initial value is set as the shift register 30 of LFSR25 (drawing 6 (d)). An initial value set as the shift register 18a is a value beforehand set up based on ID information here and an initial value set as the shift register 30 is a value determined by the LFSR initial value characteristic polynomial set part 24 by an operation based on ID information.

[0113]The code generation controller 23 of the control section 20 outputs a "shift clock" to LFSR12 and LFSR25 (drawing 6 (f)).

[0114]A "shift clock" is answered and shift operation of an  $M_1$  time is performed to the shift register 18a of LFSR12 and shift operation of an  $M_1$  time is performed to the shift register 30 of LFSR25 (drawing 6 (d)).

[0115]In LFSR12a logical operation based on [ whenever it performs one shift operation ] a LFSR specific polynomial is performed. The LFSR characteristic polynomial is a polynomial beforehand set up based on ID information. The logical operation result is fed back to an input of the shift register 18a. Similarly in LFSR25a logical operation based on [ whenever it performs one shift operation ] a LFSR specific polynomial is performed. The LFSR characteristic polynomial is a polynomial determined by the LFSR initial value characteristic polynomial set part 24 by an operation based on ID information. The logical operation result is fed back to an input of the shift register 30.

[0116]Thus in LFSR12 and 25 whenever a "shift clock" is inputted shift operation and a logical operation are repeated. As a result in encryption/decryption machines 11 and 22 the same operation is completely performed.

[0117]Thus a circuit for realizing an initial value and a LFSR characteristic polynomial for generating a pseudo-random number beforehand determined based on ID information is beforehand included in LFSR12. Structure which can form LFSR12 and equivalent logic is beforehand prepared for LFSR25 and based on ID information transmitted from the memory storage 1 the LFSR initial value characteristic polynomial set part 24 constitutes LFSR25 so that LFSR12 and equivalent logic may be formed.

[0118]As a result it is generated according to logic with equivalent the encryption / decryption KEY in encryption/decryption machine 11 and the encryption/decryption KEY in encryption/decryption machine 22.

[0119]The code generation controller 23 of the control section 20 outputs a "KEY set clock" to Key\_Reg14 and Key\_Reg27 after only the predetermined number of times outputs a "shift clock" to LFSR12 and LFSR25 (drawing 6 (c)).

[0120]While answering a "KEY set clock" incorporating into Key\_Reg14 the output data OUT outputted from LFSR12 and being held there output data SOUT outputted from LFSR25 is incorporated into Key\_Reg27 and is held there.

[0121] Thus same encryption / decryption KEY (for example  $A_1$ ) will be held Key\_Reg14 and Key\_Reg27 (drawing 6 (a)).

[0122] When the data processing device 2 is equipped with the memory storage 1 encryption/decryption machine 11 and encryption/decryption machine 22 are connected via a data bus and an address bus. Data enciphered based on encryption / decryption KEY is transmitted to the data processing device 2 from the memory storage 1 via a data bus (drawing 6 (j)). An address enciphered based on encryption / decryption KEY is transmitted to the memory storage 1 from the data processing device 2 via an address bus (drawing 6 (k)).

[0123] Then the treating part 21 outputs an address which specifies data which should be processed by the data processing device 2 among data memorized by the memory storage 1. The address is given to the encryption EOR gate sequence 29 of encryption/decryption machine 22.

[0124] The encryption EOR gate sequence 29 enciphers an address by performing an EOR operation to each bit of an address and each bit of the encryption / decryption KEY currently held Key\_Reg27. Specifically logic (1/0) of a bit of an address corresponding to a bit of two or more bits "1" of encryption / decryption KEY is reversed. An enciphered address is given to the decryption EOR gate sequence 15 of encryption/decryption machine 11.

[0125] The decryption EOR gate sequence 15 decrypts an enciphered address by performing an EOR operation to each bit of an enciphered address and each bit of the encryption / decryption KEY currently held Key\_Reg14. Specifically logic (1/0) of a bit of an enciphered address corresponding to a bit of two or more bits "1" of encryption / decryption KEY is reversed.

[0126] The encryption / decryption KEY currently held Key\_Reg14 and the encryption/decryption KEY currently held Key\_Reg27 are the same. Therefore an enciphered address is changed into the original address by decrypting an address enciphered in a mode mentioned above.

[0127] An address outputted from the decryption EOR gate sequence 15 is given to the selector 16. The selector 16 judges whether it is in a state where encryption / decryption KEY is reset. When data currently held Key\_Reg14 is except "ALL0" it judges with the selector 16 not being in a state where encryption / decryption KEY is reset. In this case the selector 16 outputs an address outputted from the decryption EOR gate sequence 15 to the storage parts store 10.

[0128] The storage parts store 10 reads data memorized by position corresponding to an address and outputs read data to the encryption EOR gate sequence 17.

[0129] The encryption EOR gate sequence 17 enciphers data outputted from the storage parts store 10 by performing an EOR operation to each bit of data outputted from the storage parts store 10 and each bit of the encryption / decryption KEY currently held Key\_Reg14. Specifically logic (1/0) of a bit of data corresponding to a bit of two or more bits "1" of encryption / decryption KEY is reversed. A principle of encryption by the encryption EOR gate sequence 17 is the same as a principle of encryption by the encryption EOR gate sequence 29.

Enciphered data is given to the decryption EOR gate sequence 28 of encryption/decryption machine 22.

[0130]The decryption EOR gate sequence 28 decrypts enciphered data by performing an EOR operation to each bit of enciphered data and each bit of the encryption / decryption KEY currently held Key\_Reg27. Specifically logic (1/0) of a bit of enciphered data corresponding to a bit of two or more bits "1" of encryption / decryption KEY is reversed. A principle of decryption by the decryption EOR gate sequence 28 is the same as a principle of decryption by the decryption EOR gate sequence 15. Data outputted from the decryption EOR gate sequence 28 is given to the treating part 21.

[0131]The treating part 21 carries out predetermined processing to data outputted from the decryption EOR gate sequence 28.

[0132]Henceforth an operation for generating new encryption / decryption KEY in parallel to a data transfer between the memory storage 1 and the data processing device 2 is performed in LFSR12 and LFSR25. Such an operation may be performed for every fixed time and may be performed for every random time.

[0133]The number of times (for example  $M_2$  time) of shift operation made in LFSR12 and LFSR25 in order to generate new encryption / decryption KEY is set up differ from the number of times (for example  $M_1$  time) of shift operation made in LFSR12 and LFSR25 in order to generate last encryption / decryption KEY (drawing 6 (d)).

[0134]A "KEY set clock" is answered and the encryption / decryption KEY currently held Key\_Reg14 and Key\_Reg27 are updated (drawing 6 (a)). Then data enciphered as an address enciphered based on new encryption / decryption KEY is transmitted between the memory storage 1 and the data processing device 2 (drawing 6 (j) drawing 6 (k)).

[0135]Thus the encryption / decryption KEY held Key\_Reg14 of encryption/decryption machine 11 and the encryption/decryption KEY held Key\_Reg27 of encryption/decryption machine 22 answer a "KEY set clock" Simultaneous moreover it is updated by momentary and new encryption / decryption KEY. Therefore also when rewriting encryption / decryption KEY it is not necessary to interrupt data transfer and data transfer can be continuously carried out between the memory storage 1 and the data processing device 2.

[0136]this invention may be boiled not only in an above-mentioned embodiment but variously and may be changed. Although all the addresses and data other than ID information are enciphered and transmitted in the above-mentioned embodiment In order to avoid unusual operation of a system when the inaccurate memory storage 1 is connected to the data processing device 2 at the time of data requestssuch as a fundamental program area it may not be made not to perform an address and a data encryption.

[0137]Although the data processing device 2 was the composition that only the one memory storage 1 was connected and data was processed in the above-mentioned embodiment It may encipher / be made to decrypt only data transmitted among the one memory storage 1 which connection of two or more memory

storage 1 was simultaneously possible and was chosen from two or more memory storage 1 to the data processing device 2.

[0138] Although he is trying to memorize peculiar ID information to the memory storage 1 in the above-mentioned embodiment to "the 0th address" of the storage parts store 10 of the memory storage 1 it may be made to provide a portion which stores ID information in addition to storage parts store 10 of the memory storage 1.

[0139] ID information peculiar to the memory storage 1 may be what kind of thing as long as it is usable for setting up not only ID numbers such as a lot number but an initial value and a characteristic polynomial of LFSR.

[0140]

[Effect of the Invention] According to the data transfer system of this invention the address and data which are transmitted between memory storage and a data processing device are enciphered. For this reason it is not easy to get to know the contents of the data memorized by memory storage from data transmitting. The data memorized by memory storage can be prevented from being reproduced unjustly by this.

[0141] According to the data transfer system of this invention the encryption / decryption KEY used for encryption and decryption of data transmitting are generated so that it may correspond to the ID information of the memory storage with which the data processing device was equipped. For this reason even if the data memorized by memory storage is reproduced as it is Encryption / decryption KEY is generated based on the ID information of memory storage and unless the structure which enciphers data based on encryption / decryption KEY is added the data processing device cannot read the duplication data correctly. It can prevent that duplicate use of the data memorized by memory storage is carried out unjustly by this.

[0142] The initial value and characteristic polynomial for generating encryption / decryption KEY based on ID information are beforehand made as a circuit by memory storage. Thereby the circuit for generating an initial value and a characteristic polynomial etc. become unnecessary. As a result small-scale-ization of memory storage is realizable.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1] It is a figure showing the example of composition of the data transfer system 100 of an embodiment of the invention.

[Drawing 2] It is a figure showing the example of composition of encryption/decryption machine 11 of the memory storage 1.

[Drawing 3] It is a figure showing the example of composition of LFSR 12.

[Drawing 4] It is a figure showing the example of composition of encryption/decryption machine 22 of the data processing device 2.

[Drawing 5]The figure in which (a) shows the example of composition of the shift register 30 and the LFSR feedback equivalent logic formation part 31and (b) are the figures showing the example of composition of the gate element 33 for LFSR feedback equivalent logic formation.

[Drawing 6]It is a timing chart explaining operation of the data transfer system 100.

[Description of Notations]

- 1 Memory storage
  - 2 Data processing device
  - 10 Storage parts store
  - 11 Encryption/decryption machine
  - 12 LFSR
  - 14 Key\_Reg
  - 15 Decryption EOR gate sequence
  - 16 Selector
  - 17 Encryption EOR gate sequence
  - 20 Control section
  - 21 Treating part
  - 22 Encryption/decryption machine
  - 23 Code generation controller
  - 24 LFSR initial value characteristic polynomial set part
  - 25 LFSR
  - 27 Key\_Reg
  - 28 Decryption EOR gate sequence
  - 29 Encryption EOR gate sequence
  - 30 Shift register
  - 31 LFSR feedback equivalent logic formation part
  - 32 A D flip-flop with set-reset
  - 33 The gate element for LFSR feedback equivalent logic formation
  - 34 EOR arithmetic element
  - 35 4-1 selector
  - 36 ID\_Reg
-

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-91828

(P2002-91828A)

(43) 公開日 平成14年3月29日 (2002. 3. 29)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード* (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 B 0 1 7
1/00		G 0 9 C 1/00	6 5 0 B 5 B 0 7 6
G 0 9 C 1/00	6 5 0		6 6 0 D 5 D 0 4 4
	6 6 0	G 1 1 B 20/10	H 5 J 1 0 4
G 1 1 B 20/10		G 0 6 F 9/06	6 6 0 L
審査請求 未請求 請求項の数19 O L (全 15 頁)			

(21) 出願番号 特願2000-282720(P2000-282720)

(22) 出願日 平成12年9月18日 (2000. 9. 18)

(71) 出願人 000005049

シャープ株式会社

大阪府大阪市阿倍野区長池町22番22号

(72) 発明者 河 範昭

大阪府大阪市阿倍野区長池町22番22号 シ

ャープ株式会社内

(74) 代理人 100078282

弁理士 山本 秀策

Fターム(参考) 5B017 AA06 BA07 CA14

5B076 FA05 FA10

5D044 AB02 AB05 AB07 BC08 CC08

DE50 GK17 HL08

5J104 AA01 AA07 AA16 EA04 EA26

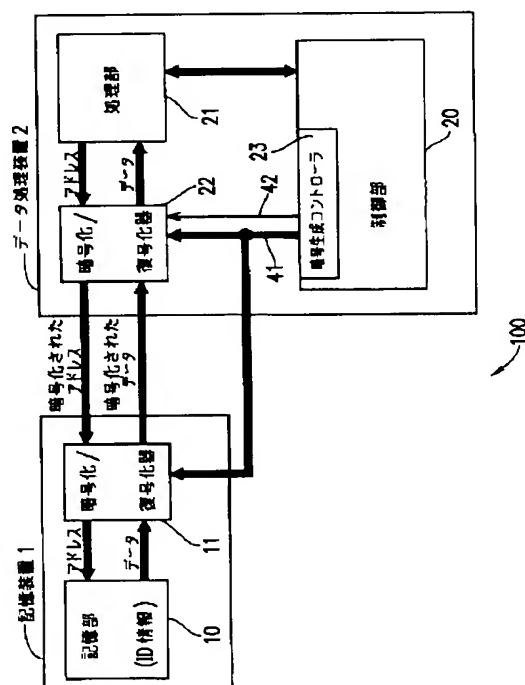
KA04 NA02 NA05 NA41 PA14

(54) 【発明の名称】 データ処理装置および記憶装置、並びに、それらを使用したデータ転送システム

(57) 【要約】

【課題】 記憶装置に記憶されているデータが不正に複製されることを確実に防止する。

【解決手段】 データ処理装置2は、記憶装置1に記憶されたデータのうちデータ処理装置2によって処理されるべきデータを指定するアドレスを出力する処理部21と、処理部21から出力されたアドレスを暗号化し、暗号化されたアドレスを記憶装置1に送り、記憶装置1から暗号化されたデータを受け取り、暗号化されたデータを復号化する暗号化/復号化器22とを備えている。暗号化/復号化器22は、記憶装置1から記憶装置1に固有のID情報を受け取り、ID情報に基づいて初期値と論理演算とを設定する設定部(36、24)と、設定された初期値に対して設定された論理演算を行うことにより、暗号化/復号化KEYを生成する暗号化/復号化KEY生成部(25、27)と、暗号化/復号化KEYに基づいてアドレスを暗号化する暗号化部29と、暗号化/復号化KEYに基づいて暗号化されたデータを復号化する復号化部28とを含む。



**【特許請求の範囲】**

**【請求項1】** 記憶装置を着脱可能なデータ処理装置であって、前記記憶装置に記憶されたデータのうち前記データ処理装置によって処理されるべきデータを指定するアドレスを出力する処理部と、前記処理部から出力された前記アドレスを暗号化し、前記暗号化されたアドレスを前記記憶装置に送り、前記記憶装置から暗号化されたデータを受け取り、前記暗号化されたデータを復号化する暗号化／復号化器とを備え、前記暗号化／復号化器は、前記記憶装置から前記記憶装置に固有のID情報を受け取り、前記ID情報に基づいて初期値と論理演算とを設定する設定部と、前記設定された初期値に対して前記設定された論理演算を行うことにより、暗号化／復号化KEYを生成する暗号化／復号化KEY生成部と、前記暗号化／復号化KEYに基づいて前記アドレスを暗号化する暗号化部と、前記暗号化／復号化KEYに基づいて前記暗号化されたデータを復号化する復号化部とを含む、データ処理装置。

**【請求項2】** 前記設定部は、前記記憶装置が前記データ処理装置に装着された際に、前記ID情報を暗号化されていない状態で受け取る、請求項1に記載のデータ処理装置。

**【請求項3】** 前記暗号化／復号化KEY生成部は、定期的または不定期的に前記暗号化／復号化KEYを更新する、請求項1に記載のデータ処理装置。

**【請求項4】** 前記暗号化部は、前記暗号化／復号化KEYと前記アドレスとに対して排他的論理和（EOR）演算を行うことにより、前記アドレスを暗号化し、前記復号化部は、前記暗号化／復号化KEYと前記暗号化されたデータとに対して排他的論理和（EOR）演算を行うことにより、前記暗号化されたデータを復号化する、請求項1に記載のデータ処理装置。

**【請求項5】** 前記暗号化／復号化KEY生成部は、複数のビットを含むデータを保持し、シフトクロックに従って前記データをシフトさせるシフトレジスタと、前記シフトレジスタに保持されている前記データに対して前記設定された論理演算に応じた選択的な排他的論理和（EOR）演算を行い、その演算結果を前記シフトレジスタの入力にフィードバックするフィードバック等価論理形成部とを含む、請求項1に記載のデータ処理装置。

**【請求項6】** 前記暗号化／復号化KEY生成部は、前記シフトレジスタに保持されている前記データのビット順序を所定の順序に並び替えることにより、前記暗号化／復号化KEYを生成する、請求項5に記載のデータ処理装置。

**【請求項7】** 前記暗号化／復号化KEY生成部は、前記シフトレジスタに保持されている前記データをシフトする回数を変更することにより、新たな暗号化／復号化KEYを生成する、請求項5に記載のデータ処理装置。

**【請求項8】** データ処理装置に脱着可能な記憶装置であって、データが記憶された記憶部であって、アドレスに対応するデータを出力する記憶部と、前記データ処理装置から暗号化されたアドレスを受け取り、前記暗号化されたアドレスを復号化し、前記記憶装置から出力された前記データを暗号化し、前記暗号化されたデータを前記データ処理装置に送る暗号化／復号化器とを備え、前記暗号化／復号化器は、前記記憶装置に予め設定されている前記記憶装置に固有のID情報に基づいて、暗号化／復号化KEYを生成する暗号化／復号化KEY生成部と、前記暗号化／復号化KEYに基づいて前記暗号化されたアドレスを復号化する復号化部と、前記暗号化／復号化KEYに基づいて前記記憶装置から出力された前記データを暗号化する暗号化部とを含む、記憶装置。

**【請求項9】** 前記暗号化／復号化KEY生成部は、定期的または不定期的に前記暗号化／復号化KEYを更新する、請求項8に記載の記憶装置。

**【請求項10】** 前記復号化部は、前記暗号化／復号化KEYと前記暗号化されたアドレスとに対して排他的論理和（EOR）演算を行うことにより、前記暗号化されたアドレスを復号化し、前記暗号化部は、前記暗号化／復号化KEYと前記データとに対して排他的論理和（EOR）演算を行うことにより、前記データを暗号化する、請求項8に記載の記憶装置。

**【請求項11】** 前記暗号化／復号化KEY生成部は、複数のビットを含むデータを保持し、シフトクロックに従って前記データをシフトさせるシフトレジスタと、前記シフトレジスタに保持されている前記データに対して前記ID情報に基づき予め設定されている選択的な排他的論理和（EOR）演算を行い、その演算結果を前記シフトレジスタの入力にフィードバックするフィードバック部とを含む、請求項8に記載の記憶装置。

**【請求項12】** 前記シフトレジスタに保持されている前記データは、前記ID情報に基づき予め設定されている初期値に初期化されている、請求項11に記載の記憶装置。

**【請求項13】** 前記暗号化／復号化KEY生成部は、前記シフトレジスタに保持されている前記データのビット順序を所定の順序に並び替えることにより、前記暗号化／復号化KEYを生成する、請求項11に記載の記憶装置。



【請求項 14】 前記暗号化／復号化KEY生成部は、前記シフトレジスタに保持されている前記データをシフトする回数を変更することにより、新たな暗号化／復号化KEYを生成する、請求項 11に記載の記憶装置。

【請求項 15】 前記記憶部と前記暗号化／復号化器とは、単一の半導体チップ上に形成されている、請求項 8に記載の記憶装置。

【請求項 16】 データ処理装置と、前記データ処理装置に着脱可能な記憶装置とを備えたデータ転送システムであって、前記データ処理装置は、前記記憶装置に記憶されたデータのうち前記データ処理装置によって処理されるべきデータを指定するアドレスを出力する処理部と、前記処理部から出力された前記アドレスを暗号化し、前記暗号化されたアドレスを前記記憶装置に送り、前記記憶装置から暗号化されたデータを受け取り、前記暗号化されたデータを復号化する第 1の暗号化／復号化器とを備え、前記第 1の暗号化／復号化器は、前記記憶装置から前記記憶装置に固有のID情報を受け取り、前記ID情報に基づいて初期値と論理演算とを設定する設定部と、前記設定された初期値に対して前記設定された論理演算を行うことにより、第 1の暗号化／復号化KEYを生成する第 1の暗号化／復号化KEY生成部と、前記第 1の暗号化／復号化KEYに基づいて前記アドレスを暗号化する第 1の暗号化部と、前記第 1の暗号化／復号化KEYに基づいて前記暗号化されたデータを復号化する第 1の復号化部とを含み、前記記憶装置は、データが記憶された記憶部であって、前記アドレスに対応するデータを出力する記憶部と、前記データ処理装置から暗号化されたアドレスを受け取り、前記暗号化されたアドレスを復号化し、前記記憶装置から出力された前記データを暗号化し、前記暗号化されたデータを前記データ処理装置に送る第 2の暗号化／復号化器とを備え、前記第 2の暗号化／復号化器は、前記記憶装置に予め設定されている前記記憶装置に固有のID情報に基づいて、第 2の暗号化／復号化KEYを生成する第 2の暗号化／復号化KEY生成部と、前記第 2の暗号化／復号化KEYに基づいて前記暗号化されたアドレスを復号化する第 2の復号化部と、前記第 2の暗号化／復号化KEYに基づいて前記記憶装置から出力された前記データを暗号化する第 2の暗号化部とを含む、データ転送システム。

【請求項 17】 前記第 1の暗号化／復号化KEYと、前記第 2の暗号化／復号化KEYとは、同等の論理に従って生成される、請求項 16に記載のデータ転送システ

ム。

【請求項 18】 前記データ処理装置は、前記第 1の暗号化／復号化器と前記第 2の暗号化／復号化器とを少なくとも制御する制御部をさらに備えている、請求項 16に記載のデータ転送システム。

【請求項 19】 前記制御部は、前記記憶装置が前記データ処理装置に装着された際に、前記第 1の暗号化／復号化KEYと前記第 2の暗号化／復号化KEYとをリセットし、前記ID情報に基づいて同一の前記第 1の暗号化／復号化KEYと前記第 2の暗号化／復号化KEYとが生成されるように、前記第 1の暗号化／復号化器と前記第 2の暗号化／復号化器とを制御する、請求項 18に記載のデータ転送システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データ処理装置に着脱可能な記憶装置に記憶されているプログラムやデータが不正に複製されることを防止するデータ処理装置および記憶装置、並びに、データ伝送システムに関する。

【0002】

【従来の技術】データ処理装置から取り外し可能な半導体記憶装置（例えば、ROM）は、今日、家庭用ビデオゲームカセットなどの形で大量に市場に供給されている。もし不正複製防止対策を講じないとすると、ゲームカセットの海賊版が大量に市場に出回るおそれがある。

【0003】従来、半導体記憶装置に記憶されているデータが不正に複製されることを防止する方法、あるいは、不正に複製されたデータを使用不能もしくは困難にする方法として、（1）暗号化されたデータを半導体記憶装置に記憶する方法、（2）半導体記憶装置に記憶されているデータを読み出す前に、半導体記憶装置もしくはデータ処理装置が正規のものであることを確認する認証手続きを行う方法が知られている。

【0004】例えば、特開昭 60-167033 号公報、特開昭 61-67136 号公報、特開平 5-53921 号公報は、暗号化されたデータを半導体記憶装置に記憶する方法を開示している。

【0005】また、例えば、特開平 6-168185 号公報、特許第 2698371 号公報は、半導体記憶装置が装着されるデータ処理装置が正規のものであることを確認する認証手続きを行った後に、半導体記憶装置に記憶されたデータを読み出す方法を開示している。

【0006】

【発明が解決しようとする課題】暗号化されたデータを半導体記憶装置に記憶する方法では、半導体記憶装置に記憶されたデータそのものが暗号化されているために、半導体記憶装置から読み出されたデータの改変使用やプログラムの盗用を防止することができる。しかし、この方法では、半導体記憶装置に記憶されている暗号化されたデータが不正に複製されることを防止することはでき

ない。

【0007】また、データ処理装置が正規のものであることを確認する認証手続きを行う方法では、正規でないデータ処理装置を用いて半導体記憶装置に記憶されているデータが不正に複製されることを防止することができる。しかし、この方法では、半導体記憶装置とデータ処理装置との間で転送される暗号化されていないデータを観測（プローブ）して読み取ることは可能であることから、半導体記憶装置に記憶されているデータ、プログラムの盗用を確実に防止することはできない。

【0008】なお、無線情報通信等の開かれたネットワーク上の通信を暗号化する方法も知られている。例えば、特開平6-342257号公報、特開平8-307411号公報は、LFSR（リニア・フィードバック・シフト・レジスタ）を組み合わせて発生させた疑似乱数に基づいて暗号化／復号化KEY（鍵）を生成し、この暗号化／復号化KEY（鍵）に基づいて通信データを暗号化する方法を開示している。これらの公報に記載の暗号化技術は、秘密通信に関する技術である。これらの公報には、半導体記憶装置に記憶されているデータが不正に複製されることを防止することを目的としてそのような暗号化技術を使用することは示唆されていない。

【0009】本発明は、上述した問題点を解決するためになされたものであり、データ処理装置に着脱可能な記憶装置に記憶されているプログラムやデータが不正に複製されることを防止するデータ処理装置および記憶装置、並びに、データ伝送システムを提供することを目的とする。

【0010】

【課題を解決するための手段】本発明のデータ処理装置は、記憶装置を着脱可能なデータ処理装置であって、前記記憶装置に記憶されたデータのうち前記データ処理装置によって処理されるべきデータを指定するアドレスを出力する処理部と、前記処理部から出力された前記アドレスを暗号化し、前記暗号化されたアドレスを前記記憶装置に送り、前記記憶装置から暗号化されたデータを受け取り、前記暗号化されたデータを復号化する暗号化／復号化器とを備え、前記暗号化／復号化器は、前記記憶装置から前記記憶装置に固有のID情報を受け取り、前記ID情報に基づいて初期値と論理演算とを設定する設定部と、前記設定された初期値に対して前記設定された論理演算を行うことにより、暗号化／復号化KEYを生成する暗号化／復号化KEY生成部と、前記暗号化／復号化KEYに基づいて前記アドレスを暗号化する暗号化部と、前記暗号化／復号化KEYに基づいて前記暗号化されたデータを復号化する復号化部とを含み、これにより、上記目的が達成される。

【0011】前記設定部は、前記記憶装置が前記データ処理装置に装着された際に、前記ID情報を暗号化されていない状態で受け取ってもよい。

【0012】前記暗号化／復号化KEY生成部は、定期的または不定期的に前記暗号化／復号化KEYを更新してもよい。

【0013】前記暗号化部は、前記暗号化／復号化KEYと前記アドレスとに対して排他的論理和（EOR）演算を行うことにより、前記アドレスを暗号化し、前記復号化部は、前記暗号化／復号化KEYと前記暗号化されたデータとに対して排他的論理和（EOR）演算を行うことにより、前記暗号化されたデータを復号化してもよい。

【0014】前記暗号化／復号化KEY生成部は、複数のビットを含むデータを保持し、シフトクロックに従って前記データをシフトさせるシフトレジスタと、前記シフトレジスタに保持されている前記データに対して前記設定された論理演算に応じた選択的な排他的論理和（EOR）演算を行い、その演算結果を前記シフトレジスタの入力にフィードバックするフィードバック等価論理形成部とを含んでもよい。

【0015】前記暗号化／復号化KEY生成部は、前記シフトレジスタに保持されている前記データのビット順序を所定の順序に並び替えることにより、前記暗号化／復号化KEYを生成してもよい。

【0016】前記暗号化／復号化KEY生成部は、前記シフトレジスタに保持されている前記データをシフトする回数を変更することにより、新たな暗号化／復号化KEYを生成してもよい。

【0017】本発明の記憶装置は、データ処理装置に脱着可能な記憶装置であって、データが記憶された記憶部であって、アドレスに対応するデータを出力する記憶部と、前記データ処理装置から暗号化されたアドレスを受け取り、前記暗号化されたアドレスを復号化し、前記記憶装置から出力された前記データを暗号化し、前記暗号化されたデータを前記データ処理装置に送る暗号化／復号化器とを備え、前記暗号化／復号化器は、前記記憶装置に予め設定されている前記記憶装置に固有のID情報に基づいて、暗号化／復号化KEYを生成する暗号化／復号化KEY生成部と、前記暗号化／復号化KEYに基づいて前記暗号化されたアドレスを復号化する復号化部と、前記暗号化／復号化KEYに基づいて前記記憶装置から出力された前記データを暗号化する暗号化部とを含み、これにより、上記目的が達成される。

【0018】前記暗号化／復号化KEY生成部は、定期的または不定期的に前記暗号化／復号化KEYを更新してもよい。

【0019】前記復号化部は、前記暗号化／復号化KEYと前記暗号化されたアドレスとに対して排他的論理和（EOR）演算を行うことにより、前記暗号化されたアドレスを復号化し、前記暗号化部は、前記暗号化／復号化KEYと前記データとに対して排他的論理和（EOR）演算を行うことにより、前記データを暗号化しても

よい。

【0020】前記暗号化／復号化KEY生成部は、複数のビットを含むデータを保持し、シフトクロックに従って前記データをシフトさせるシフトレジスタと、前記シフトレジスタに保持されている前記データに対して前記ID情報に基づき予め設定されている選択的な排他的論理和（EOR）演算を行い、その演算結果を前記シフトレジスタの入力にフィードバックするフィードバック部とを含んでいてもよい。

【0021】前記シフトレジスタに保持されている前記データは、前記ID情報に基づき予め設定されている初期値に初期化されていてもよい。

【0022】前記暗号化／復号化KEY生成部は、前記シフトレジスタに保持されている前記データのビット順序を所定の順序に並び替えることにより、前記暗号化／復号化KEYを生成してもよい。

【0023】前記暗号化／復号化KEY生成部は、前記シフトレジスタに保持されている前記データをシフトする回数を変更することにより、新たな暗号化／復号化KEYを生成してもよい。

【0024】前記記憶部と前記暗号化／復号化器とは、単一の半導体チップ上に形成されていてもよい。

【0025】本発明のデータ転送システムは、データ処理装置と、前記データ処理装置に着脱可能な記憶装置とを備えたデータ転送システムであって、前記データ処理装置は、前記記憶装置に記憶されたデータのうち前記データ処理装置によって処理されるべきデータを指定するアドレスを出力する処理部と、前記処理部から出力された前記アドレスを暗号化し、前記暗号化されたアドレスを前記記憶装置に送り、前記記憶装置から暗号化されたデータを受け取り、前記暗号化されたデータを復号化する第1の暗号化／復号化器とを備え、前記第1の暗号化／復号化器は、前記記憶装置から前記記憶装置に固有のID情報を受け取り、前記ID情報に基づいて初期値と論理演算とを設定する設定部と、前記設定された初期値に対して前記設定された論理演算を行うことにより、第1の暗号化／復号化KEYを生成する第1の暗号化／復号化KEY生成部と、前記第1の暗号化／復号化KEYに基づいて前記アドレスを暗号化する第1の暗号化部と、前記第1の暗号化／復号化KEYに基づいて前記暗号化されたデータを復号化する第1の復号化部とを含み、前記記憶装置は、データが記憶された記憶部であって、前記アドレスに対応するデータを出力する記憶部と、前記データ処理装置から暗号化されたアドレスを受け取り、前記暗号化されたアドレスを復号化し、前記記憶装置から出力された前記データを暗号化し、前記暗号化されたデータを前記データ処理装置に送る第2の暗号化／復号化器とを備え、前記第2の暗号化／復号化器は、前記記憶装置に予め設定されている前記記憶装置に固有のID情報に基づいて、第2の暗号化／復号化KEY

Yを生成する第2の暗号化／復号化KEY生成部と、前記第2の暗号化／復号化KEYに基づいて前記暗号化されたアドレスを復号化する第2の復号化部と、前記第2の暗号化／復号化KEYに基づいて前記記憶装置から出力された前記データを暗号化する第2の暗号化部とを含み、これにより、上記目的が達成される。

【0026】前記第1の暗号化／復号化KEYと、前記第2の暗号化／復号化KEYとは、同等の論理に従って生成されてもよい。

【0027】前記データ処理装置は、前記第1の暗号化／復号化器と前記第2の暗号化／復号化器とを少なくとも制御する制御部をさらに備えていてもよい。

【0028】前記制御部は、前記記憶装置が前記データ処理装置に装着された際に、前記第1の暗号化／復号化KEYと前記第2の暗号化／復号化KEYとをリセットし、前記ID情報に基づいて同一の前記第1の暗号化／復号化KEYと前記第2の暗号化／復号化KEYとが生成されるように、前記第1の暗号化／復号化器と前記第2の暗号化／復号化器とを制御してもよい。

【0029】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態を説明する。

【0030】図1は、本発明の実施の形態のデータ転送システム100の構成例を示す。

【0031】データ転送システム100は、記憶装置1と、データ処理装置2とを含む。記憶装置1は、データ処理装置2に着脱可能に構成されている。データ処理装置2には、同一規格の複数の記憶装置から選択される1つの記憶装置1が装着される。

【0032】データ処理装置2は、装着された記憶装置1に暗号化されたアドレスを出力する。記憶装置1は、暗号化されたアドレスに対応する暗号化されたデータをデータ処理装置2に出力する。このように、記憶装置1とデータ処理装置2との間で転送されるアドレスおよびデータを暗号化することによって、転送データから記憶装置1に記憶されているデータの内容を知ることは困難になる。

【0033】記憶装置1は、例えば、ゲームプログラムや各種データが記憶された家庭用ビデオゲーム用のゲームカセットである。データ処理装置2は、例えば、家庭用ビデオゲーム機である。家庭用ビデオゲーム機は、ゲームカセットを装着するための差し込み口を有している。ゲームカセットが家庭用ビデオゲーム機の差し込み口に装着されると、ゲームカセットに記憶されているゲームプログラムや各種データが家庭用ビデオゲーム機に読み出され、家庭用ビデオゲーム機に接続されているテレビなどのディスプレイにゲーム画面が表示される。

【0034】記憶装置1は、記憶部10と、暗号化／復号化器11とを含む。記憶部10と暗号化／復号化器11とは、単一の半導体チップ（例えば、シリコンチッ

ブ)上に形成されていることが好ましい。

【0035】記憶部10には、記憶装置1に固有のID情報(例えば、ID番号)と、プログラムや各種データとが予め記憶されている。ID情報は、例えば、同一規格の記憶装置(製品)毎に割り振られる品番である。あるいは、ID情報は、複数の値から選択された値であってもよい。ID情報は、記憶部10の所定のアドレス(例えば、「0番地」)に記憶される。記憶部10は、暗号化/復号化器11からアドレスを受け取り、そのアドレスに対応する位置に記憶されているデータを暗号化/復号化器11に出力する。

【0036】なお、本明細書では、用語「データ」は、記憶部10に記憶され得る任意のタイプの情報を意味するものとし、プログラムや各種データを含む包括的な用語として理解される。

【0037】暗号化/復号化器11は、暗号化されたアドレスをデータ処理装置2から受け取り、その暗号化されたアドレスを復号化することによりアドレスを生成する。そのアドレスは、記憶部10に出力される。また、暗号化/復号化器11は、記憶部10から出力されたデータを受け取り、そのデータを暗号化することにより暗号化されたデータを生成する。その暗号化されたデータは、データ処理装置2に出力される。

【0038】データ処理装置2は、処理部21と、暗号化/復号化器22とを含む。

【0039】記憶装置1がデータ処理装置2に装着されると、記憶装置1内の暗号化/復号化器11とデータ処理装置2内の暗号化/復号化器22とは互いに電気的に接続された状態となる。例えば、暗号化/復号化器11と暗号化/復号化器22とはコネクタ(図示せず)を介して互いに電気的に接続され得る。

【0040】処理部21は、記憶装置1に記憶されているデータのうちデータ処理装置2によって処理されるべきデータを指定するアドレスを出力する。

【0041】暗号化/復号化器22は、処理部21から出力されたアドレスを受け取り、そのアドレスを暗号化することにより暗号化されたアドレスを生成する。その暗号化されたアドレスは、記憶装置1に出力される。また、暗号化/復号化器22は、記憶装置1から出力された暗号化されたデータを受け取り、その暗号化されたデータを復号化することによりデータを生成する。そのデータは、処理部21に出力される。

【0042】データ処理装置2は、暗号化/復号化器11と暗号化/復号化器22と処理部21とを制御する制御部20をさらに含んでいる。

【0043】制御部20は、暗号生成コントローラ23を含む。暗号生成コントローラ23は、暗号化/復号化器11における暗号化/復号化KEYの生成および変更のタイミングと暗号化/復号化器22における暗号化/復号化KEYの生成および変更のタイミングとが同期す

るように、暗号化/復号化器11および暗号化/復号化器22を制御する。

【0044】暗号生成コントローラ23は、暗号化/復号化器11および暗号化/復号化器22に共通の制御信号を制御信号線41を介して暗号化/復号化器11および暗号化/復号化器22に供給し、暗号化/復号化器22のみに関連する制御信号を制御信号線42を介して暗号化/復号化器22に供給する。

【0045】図2は、記憶装置1の暗号化/復号化器11の構成例を示す。

【0046】暗号化/復号化器11は、疑似乱数を生成するLFSR(Linear Feedback Shift Register)12を含む。

【0047】LFSR12は、シフトレジスタに保持されているNビットのデータのうち選択されたいくつかのビットに対して排他的論理和(Exclusive OR;以下、「EOR」という)演算を行い、その演算結果をシフトレジスタの入力にフィードバックする回路である。シフトレジスタは、例えば、Dフリップフロップ(DFP)を直列に接続することによって構成される。

【0048】シフトレジスタに保持されているNビットのデータのうちのいずれのビットに対してEOR演算を行い、その演算結果をシフトレジスタのいずれのビット位置にフィードバックするかにより、特性の異なる最大 $2^N - 1$ の周期の疑似乱数(パターン)列を得ることができる。ここで、最大である $2^N - 1$ の周期を有する疑似乱数列は、一般に、「M系列(Maximum Length Sequences)」と呼ばれる。ここで、Nは2以上の任意の整数である。

【0049】なお、シフトレジスタに保持されているNビットのデータのうちのいずれのビットに対してEOR演算を行うかは、(数1)に示されるN次の多項式によって表すことができる。

【0050】

【数1】

$$f(x) = \sum_{k=0}^n a_k x^k \quad \dots (1)$$

ただし、シフトレジスタに保持されているNビットのデータのうちk番目のビットをEOR演算に使用する場合は $a_k = 1$ 、シフトレジスタに保持されているNビットのデータのうちk番目のビットをEOR演算に使用しない場合は $a_k = 0$ とし、 $a_0 = 1$ および $a_N = 1$ とされる。この多項式 $f(x)$ は、LFSR特性多項式と呼ばれ、LFSRが発生する疑似乱数の特性を表す。

【0051】例えば、 $N = 4$ の場合において、1番目のビットおよび4番目のビットに対してEOR演算を行う場合には、LFSR特性多項式 $f(x)$ は、「 $x^4 + x + 1$ 」と表される。

【0052】M系列を形成するためのLFSR特性多項

式は限られているが、本発明では、得られる擬似乱数列が特にM系列である必要はない。ただし、シフトレジスタに保持されるNビットのデータの初期値として、この処理を繰り返してもシフトレジスタに保持されるNビットのデータに変化が起こらないデッドループ（またはスタックステート）を起こすような値（例えば、「0・・・0（ALL0）」）を設定することは避けなければならない。

【0053】記憶部10に記憶されているID情報に基づいて、LFSRのシフトレジスタに保持されるべきNビットのデータの初期値と、LFSR特性多項式とが予め決定される。LFSR12は、その予め決定されたNビットのデータの初期値とLFSR特性多項式とを満たす回路として形成される。

【0054】図3は、LFSR12の構成例を示す。LFSR12は、Nビットのデータを保持するシフトレジスタ18aを有している。シフトレジスタ18aは、直列に接続されたN個のDフリップフロップ（DFF）18から構成されている。

【0055】LFSR12に初期値ロード信号が入力されると、シフトレジスタ18aに保持されているNビットのデータが初期化される。そのNビットのデータの初期値は、N個のレジスタ19に予め記憶されている。そのNビットのデータの初期値は、記憶部10に記憶されているID情報に基づいて予め決定されている。あるいは、そのNビットのデータの初期値は、N個のDFF18の各ビットに入力される初期値ロード信号が各ビットの非同期セットあるいは非同期リセットのいずれかに接続されている事で予め決定されている。

【0056】LFSR12にシフトクロックが入力されると、シフトレジスタ18aに保持されているNビットのデータは、順次、1ビットずつ所定の方向にシフトされる。シフト回数は、任意の回数に設定することが可能である。

【0057】記憶部10に記憶されているID情報に基づいて予め決定された選択規則に従って、シフトレジスタ18aに保持されているNビットのデータのうちのいくつかのビットが選択され、選択されたビットに対してEOR演算が行われる。そのEOR演算の結果は、シフトレジスタ18aの1番目のビット（すなわち、1段目のDFF18）の入力にフィードバックされる。図3に示される例では、シフトレジスタ18aに保持されているNビットのデータのうちの、1番目のビットと3番目のビットとに対してEOR演算が行われ、そのEOR演算の結果がシフトレジスタ18aの1番目のビットの入力にフィードバックされる。EOR演算素子13が、1番目のビットと3番目のビットとに対してEOR演算を行うために使用される。

【0058】シフトレジスタ18aに保持されるNビットのデータの初期値と、シフトレジスタ18aに保持さ

れるNビットのデータのうちのいずれのビットを選択してEOR演算を行うかを規定する選択規則とは、記憶部10に記憶されているID情報に基づいて一義的に決定される。

【0059】LFSR12は、暗号生成コントローラ23から供給されるシフトクロックに同期して、ランダムに設定される演算回数Mだけ、シフトレジスタ18aのシフト演算およびEOR演算を繰り返す。繰り返し処理の終了後、シフトレジスタ18aに含まれるN個のDFF18から出力されるNビットのデータが出力データOUTとしてLFSR12から出力される。出力データOUTは、疑似乱数を表す。

【0060】図2を再び参照して、レジスタ（Key\_Reg）14は、LFSR12から出力される出力データOUTのビット順序を所定のビット順序に並び替えるようにLFSR12に接続されている。Key\_Reg14に保持されるNビットのデータが、暗号化／復号化KEYとされる。

【0061】なお、LFSR12から出力される出力データOUTのビット幅とKey\_Reg14のビット幅とは、記憶部10に入力されるアドレスのビット幅および記憶部10から出力されるデータのビット幅のうち大きい方と同じもしくはそれ以上となっている。従って、Key\_Reg14に保持されるNビットのデータのうちの、アドレスのビット幅またはデータのビット幅に応じて選択されたビットのデータが暗号化／復号化KEYとされ得る。

【0062】Key\_Reg14には、暗号生成コントローラ23からKEYリセット信号およびKEYセットクロックが供給される。KEYリセット信号に同期して、Key\_Reg14に保持されている暗号化／復号化KEYがリセットされる。KEYセットクロックに同期して、LFSR12から出力される出力データOUTがKey\_Reg14に取り込まれ、保持される。

【0063】KEYセットクロックは、暗号生成コントローラ23から定期的または不定期的に出力される。暗号化／復号化KEYは、KEYセットクロックにตอบสนองして、定期的または不定期的に更新される。

【0064】このように、LFSR12およびKey\_Reg14は、記憶装置1に予め設定されている記憶装置1に固有のID情報に基づいて、暗号化／復号化KEYを生成する暗号化／復号化KEY生成部として機能する。

【0065】Key\_Reg14に保持される暗号化／復号化KEYは、復号化EORゲート列15と暗号化EORゲート列17とに与えられる。

【0066】復号化EORゲート列15は、暗号化されたアドレスをデータ処理装置2から受け取り、暗号化／復号化KEYをKey\_Reg14から受け取り、暗号化されたアドレスの各ビットと暗号化／復号化KEYの

各ビットとに対してEOR演算を行うことにより、暗号化されたアドレスを復号化する。

【0067】このように、復号化EORゲート列15は、暗号化／復号化KEYに基づいて暗号化されたアドレスを復号化する復号化部として機能する。

【0068】復号化EORゲート列15によるEOR演算結果は、セクタ16に与えられる。セクタ16は、Key\_Reg14に保持されている暗号化／復号化KEYを参照して、暗号化／復号化KEYが「ALL0」（すべてのビットが「0」であり、暗号化／復号化KEYが設定されていない状態）である場合には、「0番地」のアドレスを記憶部10に出力し、暗号化／復号化KEYが「ALL0」でない場合には、復号化EORゲート列15から出力されるアドレスを記憶部10に出力する。

【0069】記憶部10は、セクタ16から出力されるアドレスに対応する位置に格納されているデータを出力する。

【0070】暗号化EORゲート列17は、記憶部10から出力されたデータを受け取り、暗号化／復号化KEYをKey\_Reg14から受け取り、記憶部10から出力されたデータの各ビットと暗号化／復号化KEYの各ビットとに対してEOR演算を行うことにより、記憶部10から出力されたデータを暗号化する。

【0071】このように、暗号化EORゲート列17は、暗号化／復号化KEYに基づいて記憶部10から出力されたデータを暗号化する暗号化部として機能する。

【0072】上述したように、Key\_Reg14に保持されている暗号化／復号化KEYが「ALL0」である場合には、セクタ16は、復号化EORゲート列15から出力されるアドレスにかかわらず、「0番地」のアドレスを記憶部10に出力する。記憶部10は、「0番地」のアドレスに対して「0番地」に記憶されているID情報を出力する。この場合、暗号化EORゲート列17は、「ALL0」とID情報とに対してEOR演算を行うことになる。その結果、暗号化EORゲート列17からID情報が出力される。

【0073】図4は、データ処理装置2の暗号化／復号化器22の構成例を示す。

【0074】暗号化／復号化器22は、記憶装置1から出力されたID情報を保持するレジスタ(ID\_Reg)36と、ID\_Reg36に保持されたID情報に基づいて、疑似乱数を生成するための初期値とLFSR特性多項式とを決定するLFSR初期値特性多項式設定部24とを含む。

【0075】記憶装置1がデータ処理装置2に装着されると、記憶装置1からデータ処理装置2にID情報が転送される。このID情報は、暗号化されていない状態で転送される。

【0076】ID\_Reg36は、暗号生成コントロー

ラ23から供給されるIDセット信号に同期して、記憶装置1から転送されたID情報を取り込み、保持する。

ID\_Reg36に保持されたID情報は、LFSR初期値特性多項式設定部24に出力される。

【0077】LFSR初期値特性多項式設定部24において、ID情報に基づいて疑似乱数を生成するための初期値とLFSR特性多項式とを決定する際に使用される論理は、記憶装置1の暗号化／復号化器11に設けられたLFSR12において、ID情報に基づいて疑似乱数を生成するための初期値とLFSR特性多項式とを予め決定する際に使用された論理と同等である。LFSR12では、ID情報に基づき予め決定された疑似乱数を生成するための初期値とLFSR特性多項式とを実現する回路がLFSR12内に作り込まれているのに対し、LFSR初期値特性多項式設定部24では、ID情報に基づき決定された疑似乱数を生成するための初期値とLFSR特性多項式とを示す制御信号SELBUSがLFSR25に出力される。

【0078】LFSR25は、シフトレジスタ30と、LFSRフィードバック等価論理形成部31とを含む。

【0079】図5(a)は、シフトレジスタ30およびLFSRフィードバック等価論理形成部31の構成例を示す。

【0080】LFSR初期値特性多項式設定部24によって決定された疑似乱数を生成するための初期値は、シフトレジスタ30に保持されるNビットのデータの初期値としてシフトレジスタ30に設定される。

【0081】LFSRフィードバック等価論理形成部31は、LFSR特性多項式と等価な論理合成ゲートを形成するための複数のLFSRフィードバック等価論理形成用ゲート素子33を有している。複数のLFSRフィードバック等価論理形成用ゲート素子33のそれぞれは、入力端子Aと、入力端子Bと、出力端子Yと、セレクト信号入力端子Sとを有している。

【0082】図5(b)は、LFSRフィードバック等価論理形成用ゲート素子33の構成例を示す。LFSRフィードバック等価論理形成用ゲート素子33は、EOR演算素子34と、4-1セクタ35とを含む。

【0083】4-1セクタ35は、セレクト信号入力端子Sに入力されるセレクト信号に従って、4つの入力信号のうちの1つを選択する。4つの入力信号は、入力端子Aから入力される信号、入力端子Bから入力される信号、入力端子Aから入力される信号と入力端子Bから入力される信号とに対してEOR演算素子34によるEOR演算を行った結果を示す信号、論理φを示す信号である。4-1セクタ35によって選択された信号は、出力端子Yから出力される。

【0084】セレクト信号は、LFSR初期値特性多項式設定部24から出力される制御信号SELBUSの一部である。セレクト信号は、LFSR初期値特性多項式



設定部24によって決定されたLFSR特性多項式に基づいている。

【0085】図5(a)を再び参照して、LFSRフィードバック等価論理形成部31は、ピラミッド型の複数の階層に配列された複数のLFSRフィードバック等価論理形成用ゲート素子33を含む。その複数の階層の最下位層には、 $N/2$ 個のLFSRフィードバック等価論理形成用ゲート素子33が並列に並び、隣接する2つのLFSRフィードバック等価論理形成用ゲート素子33の出力端子Yからの出力が、上位層のLFSRフィードバック等価論理形成用ゲート素子33の入力端子Aおよび入力端子Bに入力される。

【0086】LFSRフィードバック等価論理形成部31は、暗号生成コントローラ23から供給される初期値ロード信号に同期して、LFSR初期値特性多項式設定部24によって決定された疑似乱数を発生させるための初期値をシフトレジスタ30に設定する。

【0087】シフトレジスタ30は、直列に接続されたN個のセットリセット付きDフリップフロップ(DFF)32から構成されている。

【0088】シフトレジスタ30にシフトクロックが入力されると、シフトレジスタ30に保持されているNビットのデータは、順次、1ビットずつ所定の方にシフトされる。例えば、シフトクロックに同期して、K番目のDFF32に保持されていたビットは、 $(K+1)$ 番目のDFF32にシフトされると同時に、 $(K+1)$ 番目のDFF32に保持されていたビットは、 $(K+2)$ 番目のDFF32にシフトされる。このように、シフトクロックに同期して、シフトレジスタ30に保持されるデータのすべてのビットが同時にシフトされる。

【0089】N個のDFF32から出力される出力信号SOUT(1)～(N)のそれぞれは、LFSRフィードバック等価論理形成部31の最下位層に配置されているLFSRフィードバック等価論理形成用ゲート素子33に入力される。例えば、出力信号SOUT(1)および(2)は、それぞれ、LFSRフィードバック等価論理形成用ゲート素子33の入力端子Aおよび入力端子Bに入力される。そのLFSRフィードバック等価論理形成用ゲート素子33のセレクト信号入力端子Sに入力されるセレクト信号に応じて、4-1セクタ35に入力される4つの信号のうちの1つの信号が選択される。選択された信号は、そのLFSRフィードバック等価論理形成用ゲート素子33の出力端子Yから出力される。そのLFSRフィードバック等価論理形成用ゲート素子33の出力端子Yから出力された信号は、上位層のLFSRフィードバック等価論理形成用ゲート素子33の入力端子Aまたは入力端子Bに入力される。このような処理が、LFSRフィードバック等価論理形成部31の最上位層に向かって繰り返される。その結果、最上位層の1つのLFSRフィードバック等価論理形成用ゲート素子

33から1ビットが出力される。この1ビットの値は、制御信号FINとして、シフトレジスタ30に保持されるNビットのデータのうちの1番目のビット（すなわち、1段目のDFF32）の入力にフィードバックされる。

【0090】シフトレジスタ30は、暗号生成コントローラ23から供給されるシフトクロックに同期して、ランダムに設定される演算回数Mだけ、シフトレジスタ30のシフト演算およびEOR演算を繰り返す。繰り返し処理の終了後、シフトレジスタ30に含まれるN個のDFF32から出力されるNビットのデータが出力データSOUTとしてLFSR25から出力される。出力データSOUTは、疑似乱数を表す。

【0091】なお、シフトレジスタ30に入力されるシフトクロックは、LFSR12に入力されるシフトクロックと同一の信号である。

【0092】このように、LFSR25は、LFSR12における論理演算と同等の論理演算に従って、LFSR12によって生成される疑似乱数と同等の疑似乱数を生成する。

【0093】LFSR25およびLFSR12において疑似乱数を生成するために実施されるシフト演算の回数Mは、暗号生成コントローラ23によってランダムに設定される。シフト演算の回数Mは、例えば、タイマーによって計時される時間に基づいて設定される。

【0094】図4を再び参照して、レジスタ(Key\_Reg)27は、LFSR25から出力される出力データSOUTのビット順序を所定のビット順序に並び替えるようにLFSR25に接続されている。Key\_Reg27に保持されるNビットのデータが、暗号化/復号化KEYとされる。

【0095】なお、LFSR25から出力される出力データSOUTのビット幅とKey\_Reg27のビット幅とは、処理部21から出力されるアドレスのビット幅および処理部21に入力されるデータのビット幅のうち大きい方と同じもしくはそれ以上となっている。従って、Key\_Reg27に保持されるNビットのデータのうち、アドレスのビット幅またはデータのビット幅に応じて選択されたビットのデータが暗号化/復号化KEYとされ得る。

【0096】Key\_Reg27には、暗号生成コントローラ23からKEYリセット信号およびKEYセットクロックが供給される。KEYリセット信号に同期して、Key\_Reg27に保持されている暗号化/復号化KEYがリセットされる。KEYセットクロックに同期して、LFSR25から出力される出力データSOUTがKey\_Reg27に取り込まれ、保持される。

【0097】なお、Key\_Reg27に入力されるKEYセットクロックは、Key\_Reg14に入力されるKEYセットクロックと同一の信号である。

【0098】このように、ID\_Reg 36 および LFSR 初期値特性多項式設定部 24 は、記憶装置 1 に固有の ID 情報に基づいて、初期値と論理演算とを設定する設定部として機能する。また、LFSR 25 および Key\_Reg 27 は、設定された初期値に対して設定された論理演算を行うことにより、暗号化／復号化 KEY を生成する暗号化／復号化 KEY 生成部として機能する。

【0099】Key\_Reg 27 に保持される暗号化／復号化 KEY は、復号化 EOR ゲート列 28 と暗号化 EOR ゲート列 29 とに与えられる。

【0100】復号化 EOR ゲート列 28 は、暗号化されたデータを記憶装置 1 から受け取り、暗号化／復号化 KEY を Key\_Reg 27 から受け取り、暗号化されたデータの各ビットと暗号化／復号化 KEY の各ビットとに対して EOR 演算を行うことにより、暗号化されたデータを復号化する。

【0101】このように、復号化 EOR ゲート列 28 は、暗号化／復号化 KEY に基づいて暗号化されたデータを復号化する復号化部として機能する。

【0102】暗号化 EOR ゲート列 29 は、処理部 21 から出力されたアドレスを受け取り、暗号化／復号化 KEY を Key\_Reg 27 から受け取り、処理部 21 から出力されたアドレスの各ビットと暗号化／復号化 KEY の各ビットとに対して EOR 演算を行うことにより、処理部 21 から出力されたアドレスを暗号化する。

【0103】このように、暗号化 EOR ゲート列 29 は、暗号化／復号化 KEY に基づいて処理部 21 から出力されたアドレスを暗号化する暗号化部として機能する。

【0104】次に、図 6 を参照して、記憶装置 1 とデータ処理装置 2 とを含むデータ転送システム 100 の動作を説明する。

【0105】記憶装置 1 がデータ処理装置 2 に装着されると、ハードリセットが行われる。このハードリセットにตอบสนองして、制御部 20 の暗号生成コントローラ 23 は、「KEY リセット信号」を暗号化／復号化器 22 に設けられた Key\_Reg 27 と暗号化／復号化器 11 に設けられた Key\_Reg 14 に出力する（図 6 (b)）。その結果、Key\_Reg 14 および Key\_Reg 27 に保持されるデータは、それぞれ、「ALL 0」にリセットされる（図 6 (a)）。Key\_Reg 14 および Key\_Reg 27 に保持されるデータが「ALL 0」であることは、暗号化／復号化 KEY がリセットされた状態であることを示す。

【0106】Key\_Reg 14 に「ALL 0」が保持されると、セクタ 16 は、復号化 EOR ゲート列 15 から出力されるアドレスにかかわらず、「0 番地」のアドレスを記憶部 10 に出力する。

【0107】記憶部 10 は、「0 番地」のアドレスに記憶された ID 情報を出力する。ID 情報は、暗号化 EOR

R ゲート列 17 を介してデータ処理装置 2 に転送される。

【0108】このように、暗号化／復号化 KEY がリセットされた状態と記憶部 10 の「0 番地」とを関連付けることにより、暗号化／復号化 KEY がリセットされた状態において、記憶部 10 の「0 番地」以外のアドレスからデータが読み出されるおそれがない。

【0109】制御部 20 の暗号生成コントローラ 23 は、「ID セット信号」を ID\_Reg 36 に出力する（図 6 (i)）。その結果、記憶装置 1 からデータ処理装置 2 に転送された ID 情報が ID\_Reg 36 にセットされる（図 6 (h)）とともに、LFSR 初期値特性多項式設定部 24 に出力される。

【0110】LFSR 初期値特性多項式設定部 24 は、ID 情報に基づいて、疑似乱数を生成するための初期値と LFSR 特性多項式とを決定する（図 6 (g)）。LFSR 初期値特性多項式設定部 24 は、疑似乱数を生成するための初期値と LFSR 特性多項式とを設定するための制御信号 SELBUS を LFSR フィードバック等価論理形成部 31 に出力する。

【0111】制御部 20 の暗号生成コントローラ 23 は、「初期値ロード信号」を LFSR 12 および LFSR 25 に出力する（図 6 (e)）。

【0112】「初期値ロード信号」にตอบสนองして、LFSR 12 のシフトレジスタ 18a に初期値が設定され、LFSR 25 のシフトレジスタ 30 に初期値が設定される（図 6 (d)）。ここで、シフトレジスタ 18a に設定される初期値は、ID 情報に基づき予め設定されていた値であり、シフトレジスタ 30 に設定される初期値は、ID 情報に基づき LFSR 初期値特性多項式設定部 24 によって演算により決定された値である。

【0113】制御部 20 の暗号生成コントローラ 23 は、「シフトクロック」を LFSR 12 および LFSR 25 に出力する（図 6 (f)）。

【0114】「シフトクロック」にตอบสนองして、LFSR 12 のシフトレジスタ 18a に対して M1 回のシフト演算が行われ、LFSR 25 のシフトレジスタ 30 に対して M1 回のシフト演算が行われる（図 6 (d)）。

【0115】なお、LFSR 12 では、1 回のシフト演算を行う度に、LFSR 特定多項式に基づく論理演算が行われる。その LFSR 特性多項式は、ID 情報に基づき予め設定されていた多項式である。その論理演算結果がシフトレジスタ 18a の入力にフィードバックされる。同様にして、LFSR 25 では、1 回のシフト演算を行う度に、LFSR 特定多項式に基づく論理演算が行われる。その LFSR 特性多項式は、ID 情報に基づき LFSR 初期値特性多項式設定部 24 によって演算により決定された多項式である。その論理演算結果がシフトレジスタ 30 の入力にフィードバックされる。

【0116】このように、LFSR 12 および 25 で



は、「シフトクロック」が入力される毎に、シフト演算と論理演算とが繰り返される。その結果、暗号化／復号化器11および22において全く同一の演算が行われる。

【0117】このように、LFSR12には、ID情報に基づいて予め決定される疑似乱数を生成するための初期値とLFSR特性多項式とを実現するための回路が予め組み込まれている。LFSR25には、LFSR12と等価論理を形成可能な仕組みが予め準備されており、LFSR初期値特性多項式設定部24は、記憶装置1から転送されるID情報に基づいて、LFSR12と等価論理を形成するようにLFSR25を構成する。

【0118】その結果、暗号化／復号化器11における暗号化／復号化KEYと、暗号化／復号化器22における暗号化／復号化KEYとは、同等の論理に従って生成される。

【0119】制御部20の暗号生成コントローラ23は、「シフトクロック」をLFSR12およびLFSR25に所定の回数だけ出力した後に、「KEYセットクロック」をKey\_Reg14およびKey\_Reg27に出力する(図6(c))。

【0120】「KEYセットクロック」にตอบสนองして、LFSR12から出力される出力データOUTがKey\_Reg14に取り込まれ、そこに保持されるとともに、LFSR25から出力される出力データSOUTがKey\_Reg27に取り込まれ、そこに保持される。

【0121】このようにして、Key\_Reg14とKey\_Reg27とに同一の暗号化／復号化KEY(例えば、A<sub>1</sub>”)が保持されることになる(図6(a))。

【0122】記憶装置1がデータ処理装置2に装着されている場合には、暗号化／復号化器11と暗号化／復号化器22とは、データバスとアドレスバスとを介して接続される。データバスを介して、暗号化／復号化KEYに基づいて暗号化されたデータが記憶装置1からデータ処理装置2に転送される(図6(j))。アドレスバスを介して、暗号化／復号化KEYに基づいて暗号化されたアドレスがデータ処理装置2から記憶装置1に転送される(図6(k))。

【0123】その後、処理部21は、記憶装置1に記憶されたデータのうちデータ処理装置2によって処理されるべきデータを指定するアドレスを出力する。そのアドレスは、暗号化／復号化器22の暗号化EORゲート列29に与えられる。

【0124】暗号化EORゲート列29は、アドレスの各ビットとKey\_Reg27に保持されている暗号化／復号化KEYの各ビットに対してEOR演算を行うことにより、アドレスを暗号化する。具体的には、暗号化／復号化KEYの複数のビットのうち「1」のビットに対応するアドレスのビットの論理(1/0)が反転され

る。暗号化されたアドレスは、暗号化／復号化器11の復号化EORゲート列15に与えられる。

【0125】復号化EORゲート列15は、暗号化されたアドレスの各ビットとKey\_Reg14に保持されている暗号化／復号化KEYの各ビットに対してEOR演算を行うことにより、暗号化されたアドレスを復号化する。具体的には、暗号化／復号化KEYの複数のビットのうち「1」のビットに対応する暗号化されたアドレスのビットの論理(1/0)が反転される。

【0126】Key\_Reg14に保持されている暗号化／復号化KEYとKey\_Reg27に保持されている暗号化／復号化KEYとは同一である。従って、上述した態様で暗号化されたアドレスを復号化することにより、暗号化されたアドレスは元のアドレスに変換される。

【0127】復号化EORゲート列15から出力されるアドレスは、セクタ16に与えられる。セクタ16は、暗号化／復号化KEYがリセットされている状態であるか否かを判定する。Key\_Reg14に保持されているデータが「ALL0」以外である場合には、セクタ16は、暗号化／復号化KEYがリセットされている状態ではないと判定する。この場合には、セクタ16は、復号化EORゲート列15から出力されるアドレスを記憶部10に出力する。

【0128】記憶部10は、アドレスに対応する位置に記憶されているデータを読み出し、読み出したデータを暗号化EORゲート列17に出力する。

【0129】暗号化EORゲート列17は、記憶部10から出力されたデータの各ビットとKey\_Reg14に保持されている暗号化／復号化KEYの各ビットに対してEOR演算を行うことにより、記憶部10から出力されたデータを暗号化する。具体的には、暗号化／復号化KEYの複数のビットのうち「1」のビットに対応するデータのビットの論理(1/0)が反転される。暗号化EORゲート列17による暗号化の原理は、暗号化EORゲート列29による暗号化の原理と同一である。暗号化されたデータは、暗号化／復号化器22の復号化EORゲート列28に与えられる。

【0130】復号化EORゲート列28は、暗号化されたデータの各ビットとKey\_Reg27に保持されている暗号化／復号化KEYの各ビットに対してEOR演算を行うことにより、暗号化されたデータを復号化する。具体的には、暗号化／復号化KEYの複数のビットのうち「1」のビットに対応する暗号化されたデータのビットの論理(1/0)が反転される。復号化EORゲート列28による復号化の原理は、復号化EORゲート列15による復号化の原理と同一である。復号化EORゲート列28から出力されるデータは、処理部21に与えられる。

【0131】処理部21は、復号化EORゲート列28

から出力されるデータに対して所定の処理を実施する。

【0132】以後、記憶装置1とデータ処理装置2との間におけるデータの転送と並行して、新たな暗号化／復号化KEYを生成するための演算がLFSR12およびLFSR25において行われる。このような演算は、一定の時間毎に行われてもよいし、ランダムな時間毎に行われてもよい。

【0133】新たな暗号化／復号化KEYを生成するためにLFSR12およびLFSR25においてなされるシフト演算の回数（例えば、M<sub>2</sub>回）は、前回の暗号化／復号化KEYを生成するためにLFSR12およびLFSR25においてなされるシフト演算の回数（例えば、M<sub>1</sub>回）とは異なるように設定される（図6（d））。

【0134】「KEYセットクロック」にตอบสนองして、Key\_Reg14およびKey\_Reg27に保持されている暗号化／復号化KEYが更新される（図6（a））。その後、新たな暗号化／復号化KEYに基づいて暗号化されたアドレスと暗号化されたデータとが記憶装置1とデータ処理装置2との間で転送される（図6（j））、図6（k））。

【0135】このように、暗号化／復号化器11のKey\_Reg14に保持された暗号化／復号化KEYと暗号化／復号化器22のKey\_Reg27に保持された暗号化／復号化KEYとは、「KEYセットクロック」にตอบสนองして、同時に、しかも、瞬時に、新たな暗号化／復号化KEYに更新される。従って、暗号化／復号化KEYを書き換える際にも、記憶装置1とデータ処理装置2との間でデータ転送を中断する必要がなく、連続してデータ転送することができる。

【0136】なお、本発明は、上述の実施の形態に限らず、種々に変更してもよい。上記の実施の形態では、ID情報以外のすべてのアドレスおよびデータを暗号化して転送しているが、データ処理装置2に不正な記憶装置1が接続された場合のシステムの異常な動作を回避するために、基礎的なプログラム領域などのデータ要求時には、アドレスおよびデータの暗号化を行わないようにしてもよい。

【0137】また、上記の実施の形態では、データ処理装置2は、1つの記憶装置1だけが接続されてデータが処理される構成であったが、データ処理装置2に対して、同時に複数の記憶装置1が接続可能であって、複数の記憶装置1から選択した1つの記憶装置1との間にて転送されるデータのみを暗号化／復号化するようにしてもよい。

【0138】さらに、上記の実施の形態では、記憶装置1の記憶部10の「0番地」のアドレスに記憶装置1に固有のID情報を記憶するようにしているが、記憶装置1の記憶部10以外に、ID情報を格納する部分を設けるようにしてもよい。

【0139】記憶装置1に固有のID情報は、品番等のID番号に限らず、LFSRの初期値および特性多項式を設定することに使用可能ならば、どのようなものであってもよい。

【0140】

【発明の効果】本発明のデータ転送システムによれば、記憶装置とデータ処理装置との間で転送されるアドレスおよびデータが暗号化されている。このため、転送データから記憶装置に記憶されたデータの内容を知ることが容易ではない。これにより、記憶装置に記憶されたデータが不正に複製されることを防止することができる。

【0141】また、本発明のデータ転送システムによれば、転送データの暗号化および復号化に使用される暗号化／復号化KEYは、データ処理装置に装着された記憶装置のID情報に対応するように生成される。このため、仮に記憶装置に記憶されているデータがそのまま複製されたとしても、記憶装置のID情報に基づいて暗号化／復号化KEYを生成し、暗号化／復号化KEYに基づいてデータを暗号化する仕組みを付加しない限り、データ処理装置は、その複製データを正しく読み取ることができない。これにより、記憶装置に記憶されたデータが不正に複製使用されることを防止することができる。

【0142】記憶装置には、ID情報に基づいて暗号化／復号化KEYを生成するための初期値および特性多項式が予め回路として作り込まれている。これにより、初期値および特性多項式を生成するための回路等が不要になる。その結果、記憶装置の小規模化を実現することができる。

【図面の簡単な説明】

【図1】本発明の実施の形態のデータ転送システム100の構成例を示す図である。

【図2】記憶装置1の暗号化／復号化器11の構成例を示す図である。

【図3】LFSR12の構成例を示す図である。

【図4】データ処理装置2の暗号化／復号化器22の構成例を示す図である。

【図5】（a）はシフトレジスタ30およびLFSRフィードバック等価論理形成部31の構成例を示す図、

（b）はLFSRフィードバック等価論理形成用ゲート素子33の構成例を示す図である。

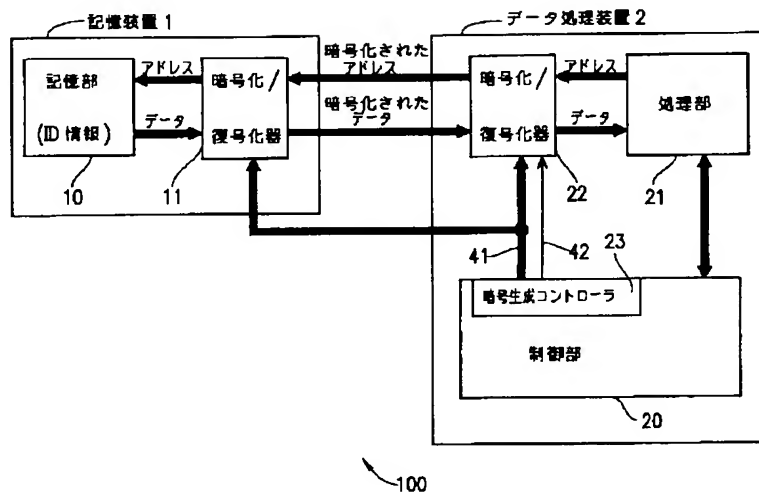
【図6】データ転送システム100の動作を説明するタイミングチャートである。

【符号の説明】

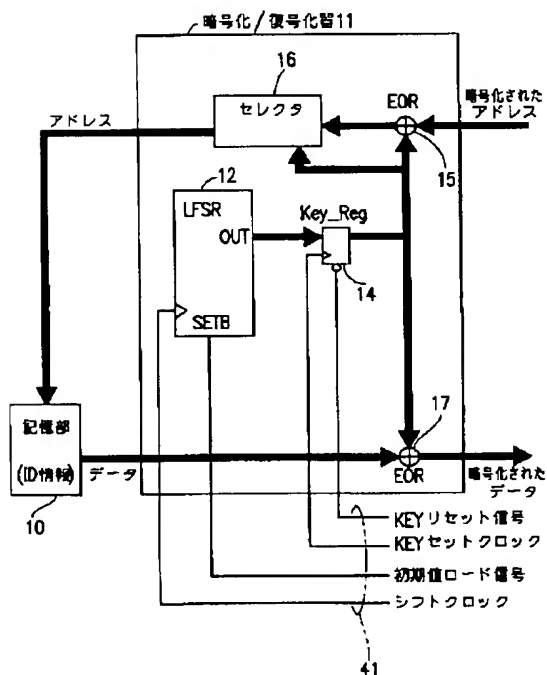
- 1 記憶装置
- 2 データ処理装置
- 10 記憶部
- 11 暗号化／復号化器
- 12 LFSR
- 14 Key\_Reg
- 15 復号化EORゲート列

- |    |                 |    |                         |
|----|-----------------|----|-------------------------|
| 16 | セレクタ            | 29 | 暗号化EORゲート列              |
| 17 | 暗号化EORゲート列      | 30 | シフトレジスタ                 |
| 20 | 制御部             | 31 | LFSRフィードバック等価論理形成部      |
| 21 | 処理部             | 32 | セットリセット付きDフリップフロップ      |
| 22 | 暗号化／復号化器        | 33 | LFSRフィードバック等価論理形成用ゲート素子 |
| 23 | 暗号生成コントローラ      | 34 | EOR演算素子                 |
| 24 | LFSR初期値特性多項式設定部 | 35 | 4-1セレクタ                 |
| 25 | LFSR            | 36 | ID_Reg                  |
| 27 | Key_Reg         |    |                         |
| 28 | 復号化EORゲート列      |    |                         |

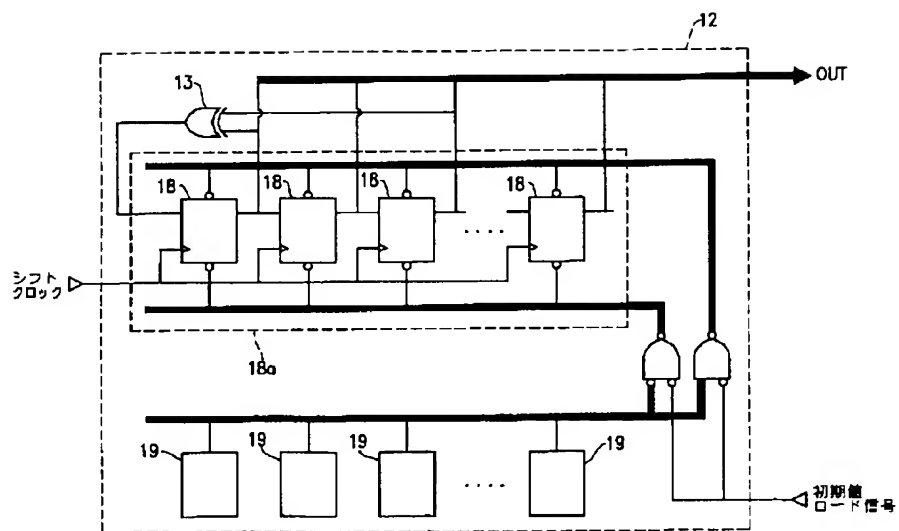
【図1】



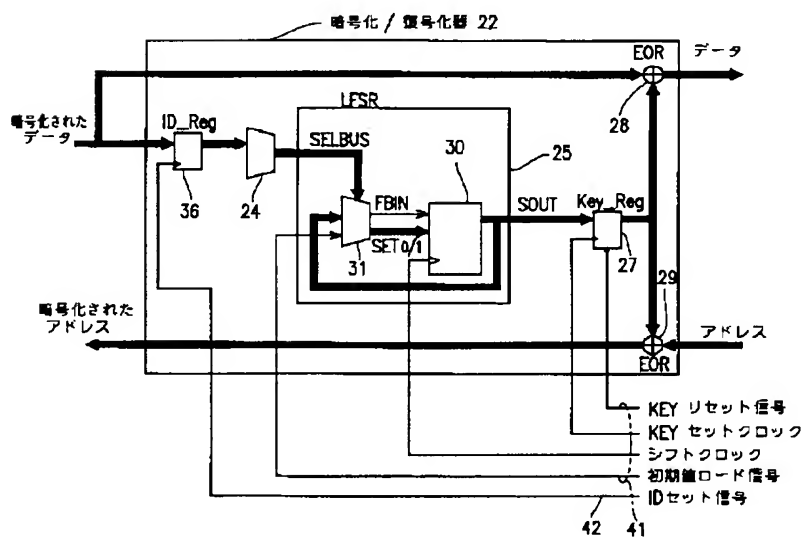
【図2】



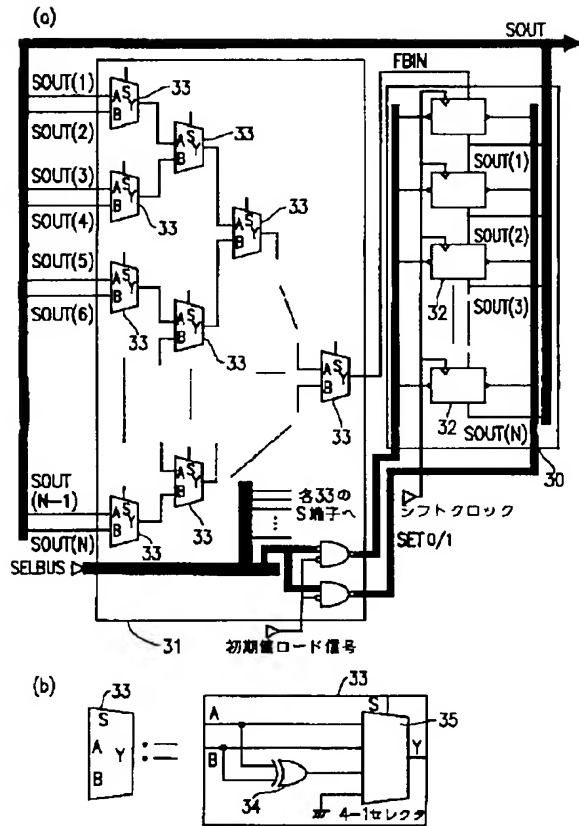
【図 3】



【図4】



【図5】



【図6】

